Unified v2.8.1 Security Updates, 2025-05-26

This document describes the 124 security updates available for Unified v2.8.1 base stations since the release, through 2025-05-26.

Date	Package	CVE(s)	Synopsys	Hardware Version
2021-09-18	libnettle4	CVE-2021-20305 CVE-2021-3580	- Non-maintainer upload by the ELTS team. - Fix CVE-2021-20305: A flaw was found in Nettle, where several Nettle signature verification functions (EDDSA & ECDSA) result in the Elliptic Curve Cryptography point (ECC) multiply function being called with out-of-range scalers, possibly resulting in incorrect results. This flaw allows an attacker to force an invalid signature, causing an assertion failure or possible validation. The highest threat to this vulnerability is to confidentiality, integrity, as well as system availability. - Fix CVE-2021-3580: A flaw was found in the way nettle's RSA decryption functions handled specially crafted ciphertext. An attacker could use this flaw to provide a manipulated ciphertext leading to application crash and denial of service.	M400 M410 R100E R100NA S1600E S100
2021-10-12	libicu52	CVE-2020-21913	- Non-maintainer upload by the LTS team. - CVE-2020-21913: Prevent a potential use-after-free vulnerability in the pkg_createWithAssemblyCode function.	M400 M410 R100E R100NA S1600E S100
2021-11-29	libgmp10	CVE-2021-43618	- Non-maintainer upload by the ELTS team. - Add patch to avoid bit size overflows. (Fixes: CVE-2021-43618)	M400 M410 R100E R100NA S1600E S100
2021-12-28	python-gnupg	CVE-2018-12020	- Non-maintainer upload by the ELTS team. - Add patch to add --no-verbose to the gpg command line. (Fixes: CVE-2018-12020)	M400 M410 R100E R100NA S1600E S100
2022-01-25	lrzsz	CVE-2018-10195	- Non-maintainer upload by the ELTS Team. - CVE-2018-10195 possible sz data leak (original patch from the Fedora project)	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
2022-03-06	libsasl2-2	CVE-2022-24407	• Non-maintainer upload by the ELTS Team. • Fix _sasl_add_string • CVE-2022-24407 Escape password for SQL insert/update commands	M400 M410 R100E R100NA S1600E S100
2022-03-06	libsasl2-modules-db	CVE-2022-24407	• Non-maintainer upload by the ELTS Team. • Fix _sasl_add_string • CVE-2022-24407 Escape password for SQL insert/update commands	M400 M410 R100E R100NA S1600E S100
2022-04-10	gzip	CVE-2022-1271	• Non-maintainer upload by the ELTS team. • Add patch to avoid exploit via multi-newline file namesfix. (Fixes: CVE-2022-1271)	M400 M410 R100E R100NA S1600E S100
2022-04-10	xz-utils	CVE-2022-1271	• Non-maintainer upload by the ELTS team. • Add patch to fix fix escaping of malicious filenames. (ZDI-CAN-16587) (Fixes: CVE-2022-1271)	M400 M410 R100E R100NA S1600E S100
2022-04-10	liblzma5	CVE-2022-1271	• Non-maintainer upload by the ELTS team. • Add patch to fix fix escaping of malicious filenames. (ZDI-CAN-16587) (Fixes: CVE-2022-1271)	M400 M410 R100E R100NA S1600E S100
2022-04-28	openvpn	CVE-2017-12166 CVE-2020-15078 CVE-2022-0547	• Non-maintainer upload by the ELTS Team. • CVE-2017-12166: buffer overflow in key-method 1. • CVE-2020-15078: authentication bypass with deferred auth. • CVE-2022-0547: authentication bypass with multiple deferred auth schemes.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
2022-05-20	libldap-2.4-2	CVE-2022-29155	• Non-maintainer upload by the ELTS Team. • CVE-2022-29155 Fix back-sql injection in filter values. (ITS#9815)	M400 M410 R100E R100NA S1600E S100
2022-07-03	dpkg	CVE-2022-1664	• Dpkg::Source::Archive: Prevent directory traversal for in-place extract> Reported by Max Justicz <max@justi.cz>. Fixes CVE-2022-1664. • Dpkg::Source::Package::V2: Always fix the permissions for upstream tarballs. ○ German (Helge Kreutzmann). (Various fixes)	M400 M410 R100E R100NA S1600E S100
2022-09-11	zlib1g	CVE-2022-37434 CVE-2018-25032	• Non-maintainer upload by the ELTS Team. • CVE-2022-37434: heap buffer overflow via large gzip header extra field • Non-maintainer upload by the ELTS Security Team. • CVE-2018-25032: Fix a bug that can crash deflate on some input when using Z_FIXED	M400 M410 R100E R100NA S1600E S100
2022-09-15	libsqlite3-0	CVE-2020-35525 CVE-2019-16168	• Non-maintainer upload by the Freexian ELTS Team. • CVE-2020-35525: Prevent a potential null pointer deference issue in INTERSEC query processing. • Non-maintainer upload by the Freexian ELTS Team. • Fix CVE-2019-16168 and CVE-2019-20218.	M400 M410 R100E R100NA S1600E S100
2022-10-10	libdbus-1-3	CVE-2022-42010	• Non-maintainer upload by the ELTS Team. • Fix several denial of service issues where an authenticated attacker can crash the system bus by sending crafted messages (CVE-2022-42010, CVE-2022-42011, CVE-2022-42012)	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
2022-10-10	dbus	CVE-2022-42010	- Non-maintainer upload by the ELTS Team. - Fix several denial of service issues where an authenticated attacker can crash the system bus by sending crafted messages (CVE-2022-42010, CVE-2022-42011, CVE-2022-42012)	M400 M410 R100E R100NA S1600E S100
2022-10-13	isc-dhcp-common	CVE-2022-2928 CVE-2022-2929	- Non-maintainer upload by the ELTS Team. - CVE-2022-2928: refcount overflow. - CVE-2022-2929: memory leak.	M400 M410 R100E R100NA S1600E S100
2022-10-13	isc-dhcp-server	CVE-2022-2928 CVE-2022-2929	- Non-maintainer upload by the ELTS Team. - CVE-2022-2928: refcount overflow. - CVE-2022-2929: memory leak.	R100NA
2022-10-13	isc-dhcp-client	CVE-2022-2928 CVE-2022-2929	- Non-maintainer upload by the ELTS Team. - CVE-2022-2928: refcount overflow. - CVE-2022-2929: memory leak.	M400 M410 R100E R100NA S1600E S100
2022-10-19	libxdmcp6	CVE-2017-2625	- Install html documentation, the txt one fails to build on armel. - Really apply patch for CVE-2017-2625 by build-depending on quilt and calling dh_quilt_patch/dh_quilt_unpatch in debian/rules.	M400 M410 R100E R100NA S1600E S100
2022-11-08	libpixman-1-0	CVE-2022-44638	- CVE-2022-44638: integer overflow leading to buffer overflow write.	M400 M410 R100E R100NA S1600E S100
2022-12-27	grub-common	CVE-2022-2601	- Non-maintainer upload by the ELTS team. - Fix CVE-2022-2601 and CVE-2022-3775: Several issues were found in GRUB2’s font handling code, which could result in crashes and potentially execution of arbitrary code. These could lead to by-pass of	S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
			UEFI Secure Boot on affected systems. Further, issues were found in image loading that could potentially lead to memory overflows. Please note that some integer overflow mitigations could not be applied because of builtin GCC functions which are only available in newer Debian versions. Only system administrators should be able to change grub2 fonts. If you use the default fonts, your system is not affected.	
2023-01-16	sudo-ldap	CVE-2023-22809	• Non-maintainer upload by the ELTS Team. • CVE-2023-22809 sudoedit: do not permit editor arguments to include "--"	M400 M410 R100E R100NA S1600E S100
2023-03-04	libsnmp30	CVE-2022-4479 CVE-2022-4479 CVE-2022-4479 CVE-2022-44792 CVE-2022-24805 CVE-2022-24806 CVE-2022-24810	• Add patches to fix DoS via null pointer exception issues: ○ debian/patches/CVE-2022-4479x-1.patch: disallow SET with NULL varbind in agent/snmp_agent.c. ○ debian/patches/CVE-2022-4479x-2.patch: allow SET with NULL varbind for testing in apps/snmpset.c. ○ debian/patches/CVE-2022-4479x-3.patch: add test for NULL varbind set in testing/fulltests/default/T0142snmpv2csetnull_simple. (Fixes: CVE-2022-44792, CVE-2022-44793 • Non-maintainer upload by the ELTS Team. • snmpd_fix_bounds_checking: CVE-2022-24805, CVE-2022-24809 • snmpd_recover_set_status: CVE-2022-24806, CVE-2022-24807, CVE-2022-24808, CVE-2022-24810 • patches based on the backports of Craig Small to Bullseye	M400 M410 R100E R100NA S1600E S100
2023-03-04	libsnmp-base	CVE-2022-4479 CVE-2022-4479 CVE-2022-4479 CVE-2022-44792 CVE-2022-24805	• Add patches to fix DoS via null pointer exception issues: ○ debian/patches/CVE-2022-4479x-1.patch: disallow SET with NULL varbind in agent/snmp_agent.c. ○ debian/patches/CVE-2022-4479x-2.patch: allow SET with NULL varbind for testing in apps/snmpset.c. ○ debian/patches/CVE-2022-4479x-3.patch: add test for NULL varbind set in	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		CVE-2022-24806 CVE-2022-24810	testing/fulltests/default/T0142snmpv2csetnull_simple. (Fixes: CVE-2022-44792, CVE-2022-44793 - Non-maintainer upload by the ELTS Team. - snmpd_fix_bounds_checking: CVE-2022-24805, CVE-2022-24809 - snmpd_recover_set_status: CVE-2022-24806, CVE-2022-24807, CVE-2022-24808, CVE-2022-24810 - patches based on the backports of Craig Small to Bullseye	
2023-05-27	libfreetype6	CVE-2022-27405 CVE-2022-27406	- Non-maintainer upload by the ELTS Team. - Add upstream patches to fix multiple vulnerabilities. ○ CVE-2022-27405: segmentation violation via ft_open_face_internal() when attempting to read the value of FT_LONG face_index. ○ CVE-2022-27406: segmentation violation via FT_Request_Size() when attempting to read the value of an unguarded face size handle.	M400 M410 R100E R100NA S1600E S100
2023-06-04	cpio	CVE-2021-38185	- Non-maintainer upload by the ELTS Security Team. - debian/rules: Fix a race condition that could result in a (rare) build failure. - Non-maintainer upload by the ELTS Security Team. - CVE-2021-38185: Arbitrary code via crafted pattern file.	M400 M410 R100E R100NA S1600E S100
2023-07-24	python-werkzeug	CVE-2023-23934 CVE-2023-25577	- Non-maintainer upload by the ELTS Security Team. - CVE-2023-23934: Werkzeug will parse the cookie =*Host-test=bad as* Host-test=bad`. If a Werkzeug application is running next to a vulnerable or malicious subdomain which sets such a cookie using a vulnerable browser, the Werkzeug application will see the bad cookie value but the valid cookie key. Browsers may allow "nameless" cookies that look like =value instead of key=value. A vulnerable browser may allow a compromised application on an adjacent subdomain to exploit this to set a cookie like =__Host-test=bad for another subdomain.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
			• CVE-2023-25577: Werkzeug’s multipart form data parser will parse an unlimited number of parts, including file parts. Parts can be a small amount of bytes, but each requires CPU time to parse and may use more memory as Python data. If a request can be made to an endpoint that accesses request.data, request.form, request.files, or request.get_data(parse_form_data=False), it can cause unexpectedly high resource usage. This allows an attacker to cause a denial of service by sending crafted multipart data to an endpoint that will parse it.	
2023-08-09	systemd	CVE-2023-26604 CVE-2022-3821	• Non-maintainer upload by the ELTS team. • Fix CVE-2023-26604: systemd does not adequately block local privilege escalation for some Sudo configurations, e.g., plausible sudoers files in which the "systemctl status" command may be executed. Specifically, systemd does not set LESSSECURE to 1, and thus other programs may be launched from the less program. This presents a substantial security risk when running systemctl from Sudo, because less executes as root when the terminal size is too small to show the complete systemctl output. • Fix CVE-2022-3821: An off-by-one Error issue was discovered in Systemd in format_timespan() function of time-util.c. An attacker could supply specific values for time and accuracy that leads to buffer overrun in format_timespan(), leading to a Denial of Service. • shutdown: don’t remount,ro network filesystems.	M400 M410 R100E R100NA S1600E S100
2023-08-09	systemd-sysv	CVE-2023-26604 CVE-2022-3821	• Non-maintainer upload by the ELTS team. • Fix CVE-2023-26604: systemd does not adequately block local privilege escalation for some Sudo configurations, e.g., plausible sudoers files in which the "systemctl status" command may be executed. Specifically, systemd does not set LESSSECURE to 1, and thus other programs may be launched from the less program. This presents a substantial security risk when running systemctl from Sudo, because less executes as root when the terminal size is too small to show the complete systemctl output. • Fix CVE-2022-3821: An off-by-one Error issue was discovered in Systemd in format_timespan() function of time-util.c. An attacker could supply specific values for time and accuracy that leads to buffer overrun in format_timespan(), leading to a Denial of Service. • shutdown: don’t remount,ro network filesystems.	M400 M410 R100E R100NA S1600E S100
2023-08-09	libudev1	CVE-2023-26604 CVE-	• Non-maintainer upload by the ELTS team.	M400 M410 R100E R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
		2022-3821	• Fix CVE-2023-26604: systemd does not adequately block local privilege escalation for some Sudo configurations, e.g., plausible sudoers files in which the "systemctl status" command may be executed. Specifically, systemd does not set LESSSECURE to 1, and thus other programs may be launched from the less program. This presents a substantial security risk when running systemctl from Sudo, because less executes as root when the terminal size is too small to show the complete systemctl output. • Fix CVE-2022-3821: An off-by-one Error issue was discovered in Systemd in format_timespan() function of time-util.c. An attacker could supply specific values for time and accuracy that leads to buffer overrun in format_timespan(), leading to a Denial of Service. • shutdown: don’t remount,ro network filesystems.	S1600E S100
2023-08-09	libpam-systemd	CVE-2023-26604 CVE-2022-3821	• Non-maintainer upload by the ELTS team. • Fix CVE-2023-26604: systemd does not adequately block local privilege escalation for some Sudo configurations, e.g., plausible sudoers files in which the "systemctl status" command may be executed. Specifically, systemd does not set LESSSECURE to 1, and thus other programs may be launched from the less program. This presents a substantial security risk when running systemctl from Sudo, because less executes as root when the terminal size is too small to show the complete systemctl output. • Fix CVE-2022-3821: An off-by-one Error issue was discovered in Systemd in format_timespan() function of time-util.c. An attacker could supply specific values for time and accuracy that leads to buffer overrun in format_timespan(), leading to a Denial of Service. • shutdown: don’t remount,ro network filesystems.	M400 M410 R100E R100NA S1600E S100
2023-08-09	libsystemd0	CVE-2023-26604 CVE-2022-3821	• Non-maintainer upload by the ELTS team. • Fix CVE-2023-26604: systemd does not adequately block local privilege escalation for some Sudo configurations, e.g., plausible sudoers files in which the "systemctl status" command may be executed. Specifically, systemd does not set LESSSECURE to 1, and thus other programs may be launched from the less program. This presents a substantial security risk when running systemctl from Sudo, because less executes as root when the terminal size is too small to show the complete systemctl output. • Fix CVE-2022-3821: An off-by-one Error issue was discovered in Systemd in format_timespan() function of time-util.c. An attacker could supply specific values for time and accuracy that leads to buffer overrun in format_timespan(), leading to a Denial of Service.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
			- shutdown: don't remount,ro network filesystems.	
2023-09-23	libssh2-1	CVE-2020-22218	- Non-maintainer upload by the ELTS Team. - CVE-2020-22218 missing check in _libssh2_packet_add() allows attackers to access out of bounds memory.	M400 M410 R100E R100NA S1600E S100
2023-09-29	libcups2	CVE-2023-4504 CVE-2023-32360 CVE-2023-34241 CVE-2023-32324 CVE-2020-10001	- CVE-2023-4504 Postscript parsing heap-based buffer overflow - CVE-2023-32360 authentication issue - CVE-2023-34241 use-after-free in cupsdAcceptClient() - CVE-2023-32324 A heap buffer overflow vulnerability would allow a remote attacker to lauch a dos attack. - Non-maintainer upload by the ELTS Team. - CVE-2020-10001.patch An input validation issue might allow a malicious application to read restricted memory.	M400 M410 R100E R100NA S1600E S100
2023-10-05	libx11-data	CVE-2023-43785 CVE-2023-43786 CVE-2023-43787 CVE-2023-3138	- CVE-2023-43785: out-of-bounds memory access in _XkbReadKeySyms - CVE-2023-43786: stack exhaustion from infinite recursion in PutSubImage - CVE-2023-43787: integer overflow in XCreateImage - Add some more patches for extra hardening. - Non-maintainer upload by the ELTS Security Team. - CVE-2023-3138: Missing input validation in various functions may result in denial of service.	M400 M410 R100E R100NA S1600E S100
2023-10-05	libx11-6	CVE-2023-43785 CVE-2023-43786 CVE-2023-	- CVE-2023-43785: out-of-bounds memory access in _XkbReadKeySyms - CVE-2023-43786: stack exhaustion from infinite recursion in PutSubImage	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		43787 CVE-2023-3138	• CVE-2023-43787: integer overflow in XCreateImage • Add some more patches for extra hardening. • Non-maintainer upload by the ELTS Security Team. • CVE-2023-3138: Missing input validation in various functions may result in denial of service.	
2023-12-17	ncurses-term	CVE-2023-29491 CVE-2020-19189 CVE-2019-17594 CVE-2022-29458 CVE-2019-17595 CVE-2019-17594 CVE-2018-19211	• Non-maintainer upload by the ELTS Team. • Mitigate CVE-2023-29491: Disallow loading of custom terminfo entries in setuid/setgid programs. • Non-maintainer upload by the ELTS Team. • Cherry-pick upstream fix for CVE-2020-19189. • Add additional CVEs fixed to CVE-2019-17594.diff & CVE-2020-17595.diff. • Non-maintainer upload by the ELTS Team. • CVE-2022-29458 Avoid out-of-bounds read in convert_strings in the terminfo library. • CVE-2019-17595 Check for missing character after backslash in fmt_entry. • CVE-2019-17594 Check for invalid hashcode in _nc_find_type_entry and nc_find_entry. • CVE-2018-19211 Avoid NULL pointer dereference in _nc_parse_entry.	M400 M410 R100E R100NA S1600E S100
2023-12-17	ncurses-bin	CVE-2023-29491 CVE-2020-19189 CVE-2019-17594 CVE-2022-29458 CVE-	• Non-maintainer upload by the ELTS Team. • Mitigate CVE-2023-29491: Disallow loading of custom terminfo entries in setuid/setgid programs. • Non-maintainer upload by the ELTS Team. • Cherry-pick upstream fix for CVE-2020-19189.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		2019-17595 CVE-2019-17594 CVE-2018-19211	• Add additional CVEs fixed to CVE-2019-17594.diff & CVE-2020-17595.diff. • Non-maintainer upload by the ELTS Team. • CVE-2022-29458 Avoid out-of-bounds read in convert_strings in the terminfo library. • CVE-2019-17595 Check for missing character after backslash in fmt_entry. • CVE-2019-17594 Check for invalid hashcode in _nc_find_type_entry and nc_find_entry. • CVE-2018-19211 Avoid NULL pointer dereference in _nc_parse_entry.	
2023-12-17	libtinfo5	CVE-2023-29491 CVE-2020-19189 CVE-2019-17594 CVE-2022-29458 CVE-2019-17595 CVE-2019-17594 CVE-2018-19211	• Non-maintainer upload by the ELTS Team. • Mitigate CVE-2023-29491: Disallow loading of custom terminfo entries in setuid/setgid programs. • Non-maintainer upload by the ELTS Team. • Cherry-pick upstream fix for CVE-2020-19189. • Add additional CVEs fixed to CVE-2019-17594.diff & CVE-2020-17595.diff. • Non-maintainer upload by the ELTS Team. • CVE-2022-29458 Avoid out-of-bounds read in convert_strings in the terminfo library. • CVE-2019-17595 Check for missing character after backslash in fmt_entry. • CVE-2019-17594 Check for invalid hashcode in _nc_find_type_entry and nc_find_entry. • CVE-2018-19211 Avoid NULL pointer dereference in _nc_parse_entry.	M400 M410 R100E R100NA S1600E S100
2023-12-17	ncurses-base	CVE-2023-29491 CVE-	• Non-maintainer upload by the ELTS Team.	M400 M410 R100E R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
		2020-19189 CVE-2019-17594 CVE-2022-29458 CVE-2019-17595 CVE-2019-17594 CVE-2018-19211	• Mitigate CVE-2023-29491: Disallow loading of custom terminfo entries in setuid/setgid programs. • Non-maintainer upload by the ELTS Team. • Cherry-pick upstream fix for CVE-2020-19189. • Add additional CVEs fixed to CVE-2019-17594.diff & CVE-2020-17595.diff. • Non-maintainer upload by the ELTS Team. • CVE-2022-29458 Avoid out-of-bounds read in convert_strings in the terminfo library. • CVE-2019-17595 Check for missing character after backslash in fmt_entry. • CVE-2019-17594 Check for invalid hashcode in _nc_find_type_entry and nc_find_entry. • CVE-2018-19211 Avoid NULL pointer dereference in _nc_parse_entry.	S1600E S100
2023-12-20	libbluetooth3	CVE-2023-45866 CVE-2022-0204 CVE-2022-39176 CVE-2022-39177 CVE-2017-1000250 CVE-2019-8921 CVE-2019-8922 CVE-2021-41229	• Non-maintainer upload by the Debian ELTS Team. • CVE-2023-45866: Fix an issue where Bluetooth Human Interface Devices (HID) hosts in BlueZ may have permitted an unauthenticated peripheral to initiate and establish encrypted connections and accept keyboard reports, potentially permitting injection of HID messages despite no user actually authorising such access. • Non-maintainer upload by the ELTS team. • patches based on the work of Sylvain Beucler for Buster • CVE-2022-0204: a heap overflow vulnerability was found in bluez. An attacker with local network access could pass specially crafted files causing an application to halt or crash, leading to a denial of service. • CVE-2022-39176: BlueZ allows physically proximate attackers to obtain sensitive information because profiles/audio/avrcp.c does not validate params_len.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
			- CVE-2022-39177: BlueZ allows physically proximate attackers to cause a denial of service because malformed and invalid capabilities can be processed in profiles/audio/avdtp.c. - Non-maintainer upload by the ELTS Security Team. - CVE-2017-1000250: replace RedHat's early patch with upstream's, so as to minimize conflicts with new CVE fixes - CVE-2019-8921: SDP infoleak, the vulnerability lies in the handling of a SVC_ATTR_REQ by the SDP implementation of BlueZ. By crafting a malicious CSTATE, it is possible to trick the server into returning more bytes than the buffer actually holds, resulting in leaking arbitrary heap data. - CVE-2019-8922: SDP Heap Overflow; this vulnerability lies in the SDP protocol handling of attribute requests as well. By requesting a huge number of attributes at the same time, an attacker can overflow the static buffer provided to hold the response. - CVE-2021-41229: sdp_cstate_alloc_buf allocates memory which will always be hung in the singly linked list of cstates and will not be freed. This will cause a memory leak over time. The data can be a very large object, which can be caused by an attacker continuously sending sdp packets and this may cause the service of the target device to crash.	
2024-01-26	libjasper1	CVE-2023-51257	- Non-maintainer upload by the ELTS team. - CVE-2023-51257 fix of invalid memory write	M400 M410 R100E R100NA S1600E S100
2024-03-11	openssh-client	CVE-2023-51385 CVE-2021-41617 CVE-2023-38408 CVE-2023-38408	- Non-maintainer upload by the ELTS team. - Add debian/salsa-ci.yml using lts-team/pipeline for jessie - Fix test cert not yet valid by using cert dates after the end of jessie ELTS. Add debian/patches/test-fix-cer-not-yet-valid.patch - CVE-2023-51385: ssh(1): Ban most shell metacharacters from user and hostnames supplied via the command-line - CVE-2021-41617: Initialise correctly supplemental groups when executing an AuthorizedKeysCommand or AuthorizedPrincipalsCommand - Non-maintainer upload by the ELTS team.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
			• remote code execution relating to PKCS#11 providers ○ d/p/CVE-2023-38408-1.patch: terminate process if requested to load a PKCS#11 provider that isn't a PKCS#11 provider in ssh-pkcs11.c. ○ CVE-2023-38408	
2024-05-17	liblwres90	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341 CVE-2023-2828 CVE-2020-8625 CVE-2015-5722 CVE-2020-8622 CVE-2021-25219 CVE-2021-25214 CVE-2022-2795 CVE-2022-38177 CVE-2021-25220 CVE-2021-25220 CVE-2021-25220 CVE-2021-25219	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash). • Non-maintainer upload by the Debian ELTS Team. • CVE-2023-2828: It was discovered that the effectiveness of the cache-cleaning algorithm used in named(5) can be severely diminished by querying the resolver for specific RRsets in a certain order, effectively allowing the configured max-cache-size limit to be significantly exceeded. • Non-maintainer upload by the ELTS Team. • Build-depend on quilt, apply and clean up patches during the build. • Make CVE-2020-8625 a real patch, and unapply it from the diff.gz and from a half-applied state in .pc (looks like it had been applied with quilt, was listed in d/p/series, but there was no .patch file). • Move CVE-2015-5722.patch from ./ to debian/patches/ and apply it using quilt, unapplying it from the .diff.gz.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Use standalone CVE-2020-8622.patch from stretch, unapply it from the .diff.gz. • Move CVE-2021-25219 changes to a patch as well. Add CVE annotation to 1:9.9.5.dfsg-9+deb8u23 changelog entry. • Move changes from CVE-2021-25214, CVE-2021-25215, CVE-2021-25216 to standalone patches. • With all patches applied, there’s no diff between deb8u27 and deb8u28 up to this point, other than to the debian/ dir itself. All of these changes have been done for maintainability purpuses, so that it’s easier to know what has changed and when, and it’s easy for anyone to revert a change if it was deemed necessary, as well as for security reviews. • New security fixes addressed in this release: ○ CVE-2022-2795: degraded performance when processing large delegations. ○ CVE-2022-38177: memory leak in ECDSA verification. • Non-maintainer upload by the ELTS team. • Apply the fix for CVE-2021-25220 again but do not patch the exported libraries because the only reverse-dependency isc-dhcp is not affected. • Non-maintainer upload by the ELTS team. • The patch for CVE-2021-25220 caused a regression in the isc-dhcp-client package which prevented network configuration via the dhclient. This patch has been reverted until the regression can be properly addressed. • Non-maintainer upload by the ELTS team. • Fix CVE-2021-25220: When using forwarders, bogus NS records supplied by, or via, those forwarders may be cached and used by named if it needs to recurse for any reason, causing it to obtain and pass on potentially incorrect answers. • Non-maintainer upload by the ELTS team. • In BIND exploitation of broken authoritative servers using a flaw in response processing can cause degradation in BIND resolver performance. The way the lame cache is currently designed makes it possible for its internal data structures to grow almost infinitely, which	

Date	Package	CVE(s)	Synopsys	Hardware Version
			may cause significant delays in client query processing (CVE-2021-25219).	
2024-05-17	libdns-export100	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341 CVE-2023-2828 CVE-2020-8625 CVE-2015-5722 CVE-2020-8622 CVE-2021-25219 CVE-2021-25214 CVE-2022-2795 CVE-2022-38177 CVE-2021-25220 CVE-2021-25220 CVE-2021-25220 CVE-2021-25219	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash). • Non-maintainer upload by the Debian ELTS Team. • CVE-2023-2828: It was discovered that the effectiveness of the cache-cleaning algorithm used in named(5) can be severely diminished by querying the resolver for specific RRsets in a certain order, effectively allowing the configured max-cache-size limit to be significantly exceeded. • Non-maintainer upload by the ELTS Team. • Build-depend on quilt, apply and clean up patches during the build. • Make CVE-2020-8625 a real patch, and unapply it from the diff.gz and from a half-applied state in .pc (looks like it had been applied with quilt, was listed in d/p/series, but there was no .patch file). • Move CVE-2015-5722.patch from ./ to debian/patches/ and apply it using quilt, unapplying it from the .diff.gz. • Use standalone CVE-2020-8622.patch from stretch, unapply it from the .diff.gz.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Move CVE-2021-25219 changes to a patch as well. Add CVE annotation to 1:9.9.5.dfsg-9+deb8u23 changelog entry. • Move changes from CVE-2021-25214, CVE-2021-25215, CVE-2021-25216 to standalone patches. • With all patches applied, there’s no diff between deb8u27 and deb8u28 up to this point, other than to the debian/ dir itself. All of these changes have been done for maintainability purpuses, so that it’s easier to know what has changed and when, and it’s easy for anyone to revert a change if it was deemed necessary, as well as for security reviews. • New security fixes addressed in this release: ○ CVE-2022-2795: degraded performance when processing large delegations. ○ CVE-2022-38177: memory leak in ECDSA verification. • Non-maintainer upload by the ELTS team. • Apply the fix for CVE-2021-25220 again but do not patch the exported libraries because the only reverse-dependency isc-dhcp is not affected. • Non-maintainer upload by the ELTS team. • The patch for CVE-2021-25220 caused a regression in the isc-dhcp-client package which prevented network configuration via the dhclient. This patch has been reverted until the regression can be properly addressed. • Non-maintainer upload by the ELTS team. • Fix CVE-2021-25220: When using forwarders, bogus NS records supplied by, or via, those forwarders may be cached and used by named if it needs to recurse for any reason, causing it to obtain and pass on potentially incorrect answers. • Non-maintainer upload by the ELTS team. • In BIND exploitation of broken authoritative servers using a flaw in response processing can cause degradation in BIND resolver performance. The way the lame cache is currently designed makes it possible for its internal data structures to grow almost infinitely, which may cause significant delays in client query processing (CVE-2021-25219).	

Date	Package	CVE(s)	Synopsys	Hardware Version
2024-05-17	libbind9-90	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341 CVE-2023-2828 CVE-2020-8625 CVE-2015-5722 CVE-2020-8622 CVE-2021-25219 CVE-2021-25214 CVE-2022-2795 CVE-2022-38177 CVE-2021-25220 CVE-2021-25220 CVE-2021-25220 CVE-2021-25219	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash). • Non-maintainer upload by the Debian ELTS Team. • CVE-2023-2828: It was discovered that the effectiveness of the cache-cleaning algorithm used in named(5) can be severely diminished by querying the resolver for specific RRsets in a certain order, effectively allowing the configured max-cache-size limit to be significantly exceeded. • Non-maintainer upload by the ELTS Team. • Build-depend on quilt, apply and clean up patches during the build. • Make CVE-2020-8625 a real patch, and unapply it from the diff.gz and from a half-applied state in .pc (looks like it had been applied with quilt, was listed in d/p/series, but there was no .patch file). • Move CVE-2015-5722.patch from ./ to debian/patches/ and apply it using quilt, unapplying it from the .diff.gz. • Use standalone CVE-2020-8622.patch from stretch, unapply it from the .diff.gz. • Move CVE-2021-25219 changes to a patch as well. Add CVE annotation to 1:9.9.5.dfsg-9+deb8u23 changelog entry. • Move changes from CVE-2021-25214, CVE-2021-25215, CVE-2021-25216 to standalone patches.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
			• With all patches applied, there’s no diff between deb8u27 and deb8u28 up to this point, other than to the debian/ dir itself. All of these changes have been done for maintainability purpuses, so that it’s easier to know what has changed and when, and it’s easy for anyone to revert a change if it was deemed necessary, as well as for security reviews. • New security fixes addressed in this release: ○ CVE-2022-2795: degraded performance when processing large delegations. ○ CVE-2022-38177: memory leak in ECDSA verification. • Non-maintainer upload by the ELTS team. • Apply the fix for CVE-2021-25220 again but do not patch the exported libraries because the only reverse-dependency isc-dhcp is not affected. • Non-maintainer upload by the ELTS team. • The patch for CVE-2021-25220 caused a regression in the isc-dhcp-client package which prevented network configuration via the dhclient. This patch has been reverted until the regression can be properly addressed. • Non-maintainer upload by the ELTS team. • Fix CVE-2021-25220: When using forwarders, bogus NS records supplied by, or via, those forwarders may be cached and used by named if it needs to recurse for any reason, causing it to obtain and pass on potentially incorrect answers. • Non-maintainer upload by the ELTS team. • In BIND exploitation of broken authoritative servers using a flaw in response processing can cause degradation in BIND resolver performance. The way the lame cache is currently designed makes it possible for its internal data structures to grow almost infinitely, which may cause significant delays in client query processing (CVE-2021-25219).	
2024-05-17	libisccfg90	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868)	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		CVE-2023-3341 CVE-2023-2828 CVE-2020-8625 CVE-2015-5722 CVE-2020-8622 CVE-2021-25219 CVE-2021-25214 CVE-2022-2795 CVE-2022-38177 CVE-2021-25220 CVE-2021-25220 CVE-2021-25220 CVE-2021-25219	• Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash). • Non-maintainer upload by the Debian ELTS Team. • CVE-2023-2828: It was discovered that the effectiveness of the cache-cleaning algorithm used in named(5) can be severely diminished by querying the resolver for specific RRsets in a certain order, effectively allowing the configured max-cache-size limit to be significantly exceeded. • Non-maintainer upload by the ELTS Team. • Build-depend on quilt, apply and clean up patches during the build. • Make CVE-2020-8625 a real patch, and unapply it from the diff.gz and from a half-applied state in .pc (looks like it had been applied with quilt, was listed in d/p/series, but there was no .patch file). • Move CVE-2015-5722.patch from ./ to debian/patches/ and apply it using quilt, unapplying it from the .diff.gz. • Use standalone CVE-2020-8622.patch from stretch, unapply it from the .diff.gz. • Move CVE-2021-25219 changes to a patch as well. Add CVE annotation to 1:9.9.5.dfsg-9+deb8u23 changelog entry. • Move changes from CVE-2021-25214, CVE-2021-25215, CVE-2021-25216 to standalone patches. • With all patches applied, there’s no diff between deb8u27 and deb8u28 up to this point, other than to the debian/ dir itself. All of these changes have been done for maintainability purpuses, so that it’s easier to know what has changed and when, and it’s easy for anyone to revert a change if it was deemed necessary, as well as for security reviews. • New security fixes addressed in this release:	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ CVE-2022-2795: degraded performance when processing large delegations. ○ CVE-2022-38177: memory leak in ECDSA verification. • Non-maintainer upload by the ELTS team. • Apply the fix for CVE-2021-25220 again but do not patch the exported libraries because the only reverse-dependency isc-dhcp is not affected. • Non-maintainer upload by the ELTS team. • The patch for CVE-2021-25220 caused a regression in the isc-dhcp-client package which prevented network configuration via the dhclient. This patch has been reverted until the regression can be properly addressed. • Non-maintainer upload by the ELTS team. • Fix CVE-2021-25220: When using forwarders, bogus NS records supplied by, or via, those forwarders may be cached and used by named if it needs to recurse for any reason, causing it to obtain and pass on potentially incorrect answers. • Non-maintainer upload by the ELTS team. • In BIND exploitation of broken authoritative servers using a flaw in response processing can cause degradation in BIND resolver performance. The way the lame cache is currently designed makes it possible for its internal data structures to grow almost infinitely, which may cause significant delays in client query processing (CVE-2021-25219).	
2024-05-17	libdns100	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341 CVE-2023-2828 CVE-2020-8625 CVE-	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		2015-5722 CVE-2020-8622 CVE-2021-25219 CVE-2021-25214 CVE-2022-2795 CVE-2022-38177 CVE-2021-25220 CVE-2021-25220 CVE-2021-25220 CVE-2021-25219	• Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash). • Non-maintainer upload by the Debian ELTS Team. • CVE-2023-2828: It was discovered that the effectiveness of the cache-cleaning algorithm used in named(5) can be severely diminished by querying the resolver for specific RRsets in a certain order, effectively allowing the configured max-cache-size limit to be significantly exceeded. • Non-maintainer upload by the ELTS Team. • Build-depend on quilt, apply and clean up patches during the build. • Make CVE-2020-8625 a real patch, and unapply it from the diff.gz and from a half-applied state in .pc (looks like it had been applied with quilt, was listed in d/p/series, but there was no .patch file). • Move CVE-2015-5722.patch from ./ to debian/patches/ and apply it using quilt, unapplying it from the .diff.gz. • Use standalone CVE-2020-8622.patch from stretch, unapply it from the .diff.gz. • Move CVE-2021-25219 changes to a patch as well. Add CVE annotation to 1:9.9.5.dfsg-9+deb8u23 changelog entry. • Move changes from CVE-2021-25214, CVE-2021-25215, CVE-2021-25216 to standalone patches. • With all patches applied, there’s no diff between deb8u27 and deb8u28 up to this point, other than to the debian/ dir itself. All of these changes have been done for maintainability purpuses, so that it’s easier to know what has changed and when, and it’s easy for anyone to revert a change if it was deemed necessary, as well as for security reviews. • New security fixes addressed in this release: ○ CVE-2022-2795: degraded performance when processing large delegations. ○ CVE-2022-38177: memory leak in ECDSA verification.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Non-maintainer upload by the ELTS team. • Apply the fix for CVE-2021-25220 again but do not patch the exported libraries because the only reverse-dependency isc-dhcp is not affected. • Non-maintainer upload by the ELTS team. • The patch for CVE-2021-25220 caused a regression in the isc-dhcp-client package which prevented network configuration via the dhclient. This patch has been reverted until the regression can be properly addressed. • Non-maintainer upload by the ELTS team. • Fix CVE-2021-25220: When using forwarders, bogus NS records supplied by, or via, those forwarders may be cached and used by named if it needs to recurse for any reason, causing it to obtain and pass on potentially incorrect answers. • Non-maintainer upload by the ELTS team. • In BIND exploitation of broken authoritative servers using a flaw in response processing can cause degradation in BIND resolver performance. The way the lame cache is currently designed makes it possible for its internal data structures to grow almost infinitely, which may cause significant delays in client query processing (CVE-2021-25219).	
2024-05-17	libisccc90	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341 CVE-2023-2828 CVE-2020-8625 CVE-2015-5722 CVE-2020-8622 CVE-	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		2021-25219 CVE-2021-25214 CVE-2022-2795 CVE-2022-38177 CVE-2021-25220 CVE-2021-25220 CVE-2021-25220 CVE-2021-25219	• CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash). • Non-maintainer upload by the Debian ELTS Team. • CVE-2023-2828: It was discovered that the effectiveness of the cache-cleaning algorithm used in named(5) can be severely diminished by querying the resolver for specific RRsets in a certain order, effectively allowing the configured max-cache-size limit to be significantly exceeded. • Non-maintainer upload by the ELTS Team. • Build-depend on quilt, apply and clean up patches during the build. • Make CVE-2020-8625 a real patch, and unapply it from the diff.gz and from a half-applied state in .pc (looks like it had been applied with quilt, was listed in d/p/series, but there was no .patch file). • Move CVE-2015-5722.patch from ./ to debian/patches/ and apply it using quilt, unapplying it from the .diff.gz. • Use standalone CVE-2020-8622.patch from stretch, unapply it from the .diff.gz. • Move CVE-2021-25219 changes to a patch as well. Add CVE annotation to 1:9.9.5.dfsg-9+deb8u23 changelog entry. • Move changes from CVE-2021-25214, CVE-2021-25215, CVE-2021-25216 to standalone patches. • With all patches applied, there’s no diff between deb8u27 and deb8u28 up to this point, other than to the debian/ dir itself. All of these changes have been done for maintainability purpuses, so that it’s easier to know what has changed and when, and it’s easy for anyone to revert a change if it was deemed necessary, as well as for security reviews. • New security fixes addressed in this release: ○ CVE-2022-2795: degraded performance when processing large delegations. ○ CVE-2022-38177: memory leak in ECDSA verification. • Non-maintainer upload by the ELTS team.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- Apply the fix for CVE-2021-25220 again but do not patch the exported libraries because the only reverse-dependency isc-dhcp is not affected. - Non-maintainer upload by the ELTS team. - The patch for CVE-2021-25220 caused a regression in the isc-dhcp-client package which prevented network configuration via the dhclient. This patch has been reverted until the regression can be properly addressed. - Non-maintainer upload by the ELTS team. - Fix CVE-2021-25220: When using forwarders, bogus NS records supplied by, or via, those forwarders may be cached and used by named if it needs to recurse for any reason, causing it to obtain and pass on potentially incorrect answers. - Non-maintainer upload by the ELTS team. - In BIND exploitation of broken authoritative servers using a flaw in response processing can cause degradation in BIND resolver performance. The way the lame cache is currently designed makes it possible for its internal data structures to grow almost infinitely, which may cause significant delays in client query processing (CVE-2021-25219).	
2024-05-17	libisccfg-export90	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341 CVE-2023-2828 CVE-2020-8625 CVE-2015-5722 CVE-2020-8622 CVE-2021-25219 CVE-	- Non-maintainer upload by the ELTS Team. - CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) - Add debian/.gitlab-ci.yml using recipe for jessie - Add debian/tests/ from buster - Make d/tests/validation less flaky. - Non-maintainer upload by the ELTS Team. - CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash).	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		2021-25214 CVE-2022-2795 CVE-2022-38177 CVE-2021-25220 CVE-2021-25220 CVE-2021-25220 CVE-2021-25219	• Non-maintainer upload by the Debian ELTS Team. • CVE-2023-2828: It was discovered that the effectiveness of the cache-cleaning algorithm used in named(5) can be severely diminished by querying the resolver for specific RRsets in a certain order, effectively allowing the configured max-cache-size limit to be significantly exceeded. • Non-maintainer upload by the ELTS Team. • Build-depend on quilt, apply and clean up patches during the build. • Make CVE-2020-8625 a real patch, and unapply it from the diff.gz and from a half-applied state in .pc (looks like it had been applied with quilt, was listed in d/p/series, but there was no .patch file). • Move CVE-2015-5722.patch from ./ to debian/patches/ and apply it using quilt, unapplying it from the .diff.gz. • Use standalone CVE-2020-8622.patch from stretch, unapply it from the .diff.gz. • Move CVE-2021-25219 changes to a patch as well. Add CVE annotation to 1:9.9.5.dfsg-9+deb8u23 changelog entry. • Move changes from CVE-2021-25214, CVE-2021-25215, CVE-2021-25216 to standalone patches. • With all patches applied, there’s no diff between deb8u27 and deb8u28 up to this point, other than to the debian/ dir itself. All of these changes have been done for maintainability purpuses, so that it’s easier to know what has changed and when, and it’s easy for anyone to revert a change if it was deemed necessary, as well as for security reviews. • New security fixes addressed in this release: ○ CVE-2022-2795: degraded performance when processing large delegations. ○ CVE-2022-38177: memory leak in ECDSA verification. • Non-maintainer upload by the ELTS team. • Apply the fix for CVE-2021-25220 again but do not patch the exported libraries because the only reverse-dependency isc-dhcp is not affected. • Non-maintainer upload by the ELTS team.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• The patch for CVE-2021-25220 caused a regression in the isc-dhcp-client package which prevented network configuration via the dhclient. This patch has been reverted until the regression can be properly addressed. • Non-maintainer upload by the ELTS team. • Fix CVE-2021-25220: When using forwarders, bogus NS records supplied by, or via, those forwarders may be cached and used by named if it needs to recurse for any reason, causing it to obtain and pass on potentially incorrect answers. • Non-maintainer upload by the ELTS team. • In BIND exploitation of broken authoritative servers using a flaw in response processing can cause degradation in BIND resolver performance. The way the lame cache is currently designed makes it possible for its internal data structures to grow almost infinitely, which may cause significant delays in client query processing (CVE-2021-25219).	
2024-05-17	libirs-export91	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341 CVE-2023-2828 CVE-2020-8625 CVE-2015-5722 CVE-2020-8622 CVE-2021-25219 CVE-2021-25214 CVE-2022-2795 CVE-2022-	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash). • Non-maintainer upload by the Debian ELTS Team. • CVE-2023-2828: It was discovered that the effectiveness of the cache-cleaning algorithm used in named(5) can be severely diminished by querying the resolver for specific RRsets in a certain order, effectively	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		38177 CVE-2021-25220 CVE-2021-25220 CVE-2021-25220 CVE-2021-25219	allowing the configured max-cache-size limit to be significantly exceeded. • Non-maintainer upload by the ELTS Team. • Build-depend on quilt, apply and clean up patches during the build. • Make CVE-2020-8625 a real patch, and unapply it from the diff.gz and from a half-applied state in .pc (looks like it had been applied with quilt, was listed in d/p/series, but there was no .patch file). • Move CVE-2015-5722.patch from ./ to debian/patches/ and apply it using quilt, unapplying it from the .diff.gz. • Use standalone CVE-2020-8622.patch from stretch, unapply it from the .diff.gz. • Move CVE-2021-25219 changes to a patch as well. Add CVE annotation to 1:9.9.5.dfsg-9+deb8u23 changelog entry. • Move changes from CVE-2021-25214, CVE-2021-25215, CVE-2021-25216 to standalone patches. • With all patches applied, there’s no diff between deb8u27 and deb8u28 up to this point, other than to the debian/ dir itself. All of these changes have been done for maintainability purpuses, so that it’s easier to know what has changed and when, and it’s easy for anyone to revert a change if it was deemed necessary, as well as for security reviews. • New security fixes addressed in this release: ○ CVE-2022-2795: degraded performance when processing large delegations. ○ CVE-2022-38177: memory leak in ECDSA verification. • Non-maintainer upload by the ELTS team. • Apply the fix for CVE-2021-25220 again but do not patch the exported libraries because the only reverse-dependency isc-dhcp is not affected. • Non-maintainer upload by the ELTS team. • The patch for CVE-2021-25220 caused a regression in the isc-dhcp-client package which prevented network configuration via the dhclient. This patch has been reverted until the regression can be properly addressed.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Non-maintainer upload by the ELTS team. • Fix CVE-2021-25220: When using forwarders, bogus NS records supplied by, or via, those forwarders may be cached and used by named if it needs to recurse for any reason, causing it to obtain and pass on potentially incorrect answers. • Non-maintainer upload by the ELTS team. • In BIND exploitation of broken authoritative servers using a flaw in response processing can cause degradation in BIND resolver performance. The way the lame cache is currently designed makes it possible for its internal data structures to grow almost infinitely, which may cause significant delays in client query processing (CVE-2021-25219).	
2024-05-17	libisc95	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341 CVE-2023-2828 CVE-2020-8625 CVE-2015-5722 CVE-2020-8622 CVE-2021-25219 CVE-2021-25214 CVE-2022-2795 CVE-2022-38177 CVE-2021-25220 CVE-2021-	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash). • Non-maintainer upload by the Debian ELTS Team. • CVE-2023-2828: It was discovered that the effectiveness of the cache-cleaning algorithm used in named(5) can be severely diminished by querying the resolver for specific RRsets in a certain order, effectively allowing the configured max-cache-size limit to be significantly exceeded. • Non-maintainer upload by the ELTS Team.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		25220 CVE-2021-25220 CVE-2021-25219	• Build-depend on quilt, apply and clean up patches during the build. • Make CVE-2020-8625 a real patch, and unapply it from the diff.gz and from a half-applied state in .pc (looks like it had been applied with quilt, was listed in d/p/series, but there was no .patch file). • Move CVE-2015-5722.patch from ./ to debian/patches/ and apply it using quilt, unapplying it from the .diff.gz. • Use standalone CVE-2020-8622.patch from stretch, unapply it from the .diff.gz. • Move CVE-2021-25219 changes to a patch as well. Add CVE annotation to 1:9.9.5.dfsg-9+deb8u23 changelog entry. • Move changes from CVE-2021-25214, CVE-2021-25215, CVE-2021-25216 to standalone patches. • With all patches applied, there's no diff between deb8u27 and deb8u28 up to this point, other than to the debian/ dir itself. All of these changes have been done for maintainability purpuses, so that it's easier to know what has changed and when, and it's easy for anyone to revert a change if it was deemed necessary, as well as for security reviews. • New security fixes addressed in this release: ○ CVE-2022-2795: degraded performance when processing large delegations. ○ CVE-2022-38177: memory leak in ECDSA verification. • Non-maintainer upload by the ELTS team. • Apply the fix for CVE-2021-25220 again but do not patch the exported libraries because the only reverse-dependency isc-dhcp is not affected. • Non-maintainer upload by the ELTS team. • The patch for CVE-2021-25220 caused a regression in the isc-dhcp-client package which prevented network configuration via the dhclient. This patch has been reverted until the regression can be properly addressed. • Non-maintainer upload by the ELTS team. • Fix CVE-2021-25220: When using forwarders, bogus NS records supplied by, or via, those forwarders may be cached and used by	

Date	Package	CVE(s)	Synopsys	Hardware Version
			named if it needs to recurse for any reason, causing it to obtain and pass on potentially incorrect answers. • Non-maintainer upload by the ELTS team. • In BIND exploitation of broken authoritative servers using a flaw in response processing can cause degradation in BIND resolver performance. The way the lame cache is currently designed makes it possible for its internal data structures to grow almost infinitely, which may cause significant delays in client query processing (CVE-2021-25219).	
2024-05-17	libisc-export95	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341 CVE-2023-2828 CVE-2020-8625 CVE-2015-5722 CVE-2020-8622 CVE-2021-25219 CVE-2021-25214 CVE-2022-2795 CVE-2022-38177 CVE-2021-25220 CVE-2021-25220 CVE-2021-25220 CVE-	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash). • Non-maintainer upload by the Debian ELTS Team. • CVE-2023-2828: It was discovered that the effectiveness of the cache-cleaning algorithm used in named(5) can be severely diminished by querying the resolver for specific RRsets in a certain order, effectively allowing the configured max-cache-size limit to be significantly exceeded. • Non-maintainer upload by the ELTS Team. • Build-depend on quilt, apply and clean up patches during the build. • Make CVE-2020-8625 a real patch, and unapply it from the diff.gz and from a half-applied state in .pc (looks like it had been applied with quilt, was listed in d/p/series, but there was no .patch file).	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		2021-25219	• Move CVE-2015-5722.patch from ./ to debian/patches/ and apply it using quilt, unapplying it from the .diff.gz. • Use standalone CVE-2020-8622.patch from stretch, unapply it from the .diff.gz. • Move CVE-2021-25219 changes to a patch as well. Add CVE annotation to 1:9.9.5.dfsg-9+deb8u23 changelog entry. • Move changes from CVE-2021-25214, CVE-2021-25215, CVE-2021-25216 to standalone patches. • With all patches applied, there's no diff between deb8u27 and deb8u28 up to this point, other than to the debian/ dir itself. All of these changes have been done for maintainability purpuses, so that it's easier to know what has changed and when, and it's easy for anyone to revert a change if it was deemed necessary, as well as for security reviews. • New security fixes addressed in this release: ○ CVE-2022-2795: degraded performance when processing large delegations. ○ CVE-2022-38177: memory leak in ECDSA verification. • Non-maintainer upload by the ELTS team. • Apply the fix for CVE-2021-25220 again but do not patch the exported libraries because the only reverse-dependency isc-dhcp is not affected. • Non-maintainer upload by the ELTS team. • The patch for CVE-2021-25220 caused a regression in the isc-dhcp-client package which prevented network configuration via the dhclient. This patch has been reverted until the regression can be properly addressed. • Non-maintainer upload by the ELTS team. • Fix CVE-2021-25220: When using forwarders, bogus NS records supplied by, or via, those forwarders may be cached and used by named if it needs to recurse for any reason, causing it to obtain and pass on potentially incorrect answers. • Non-maintainer upload by the ELTS team. • In BIND exploitation of broken authoritative servers using a flaw in response processing can cause degradation in BIND resolver performance. The way the lame cache is currently designed makes it	

Date	Package	CVE(s)	Synopsys	Hardware Version
			possible for its internal data structures to grow almost infinitely, which may cause significant delays in client query processing (CVE-2021-25219).	
2024-05-17	bind9-host	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341 CVE-2023-2828 CVE-2020-8625 CVE-2015-5722 CVE-2020-8622 CVE-2021-25219 CVE-2021-25214 CVE-2022-2795 CVE-2022-38177 CVE-2021-25220 CVE-2021-25220 CVE-2021-25220 CVE-2021-25219	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash). • Non-maintainer upload by the Debian ELTS Team. • CVE-2023-2828: It was discovered that the effectiveness of the cache-cleaning algorithm used in named(5) can be severely diminished by querying the resolver for specific RRsets in a certain order, effectively allowing the configured max-cache-size limit to be significantly exceeded. • Non-maintainer upload by the ELTS Team. • Build-depend on quilt, apply and clean up patches during the build. • Make CVE-2020-8625 a real patch, and unapply it from the diff.gz and from a half-applied state in .pc (looks like it had been applied with quilt, was listed in d/p/series, but there was no .patch file). • Move CVE-2015-5722.patch from ./ to debian/patches/ and apply it using quilt, unapplying it from the .diff.gz. • Use standalone CVE-2020-8622.patch from stretch, unapply it from the .diff.gz.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Move CVE-2021-25219 changes to a patch as well. Add CVE annotation to 1:9.9.5.dfsg-9+deb8u23 changelog entry. • Move changes from CVE-2021-25214, CVE-2021-25215, CVE-2021-25216 to standalone patches. • With all patches applied, there’s no diff between deb8u27 and deb8u28 up to this point, other than to the debian/ dir itself. All of these changes have been done for maintainability purpuses, so that it’s easier to know what has changed and when, and it’s easy for anyone to revert a change if it was deemed necessary, as well as for security reviews. • New security fixes addressed in this release: ○ CVE-2022-2795: degraded performance when processing large delegations. ○ CVE-2022-38177: memory leak in ECDSA verification. • Non-maintainer upload by the ELTS team. • Apply the fix for CVE-2021-25220 again but do not patch the exported libraries because the only reverse-dependency isc-dhcp is not affected. • Non-maintainer upload by the ELTS team. • The patch for CVE-2021-25220 caused a regression in the isc-dhcp-client package which prevented network configuration via the dhclient. This patch has been reverted until the regression can be properly addressed. • Non-maintainer upload by the ELTS team. • Fix CVE-2021-25220: When using forwarders, bogus NS records supplied by, or via, those forwarders may be cached and used by named if it needs to recurse for any reason, causing it to obtain and pass on potentially incorrect answers. • Non-maintainer upload by the ELTS team. • In BIND exploitation of broken authoritative servers using a flaw in response processing can cause degradation in BIND resolver performance. The way the lame cache is currently designed makes it possible for its internal data structures to grow almost infinitely, which may cause significant delays in client query processing (CVE-2021-25219).	

Date	Package	CVE(s)	Synopsys	Hardware Version
2024-05-22	less	CVE-2022-48624	• No-change rebuild. • Non-maintainer upload by the ELTS team. • Fix CVE-2022-48624 and CVE-2024-32487: Several vulnerabilities were discovered in less, a file pager, which may result in the execution of arbitrary commands if a file with a specially crafted file name is processed.	M400 M410 R100E R100NA S1600E S100
2024-06-17	nano	CVE-2024-5742	• Non-maintainer upload by the ELTS Team. • CVE-2024-5742: Emergency file symlink attack	M400 M410 R100E R100NA S1600E S100
2024-06-30	locales	CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602 CVE-2024-2961 CVE-2015-8984 CVE-2017-12132 CVE-2017-12133 CVE-2017-15670 CVE-2017-15671 CVE-2017-15804 CVE-2017-16997 CVE-2017-1000408 CVE-2017-	• Non-maintainer upload by the ELTS Team. • CVE-2024-33599: nscd: Stack-based buffer overflow in netgroup cache • CVE-2024-33600: nscd: Null pointer crashes after notfound response • CVE-2024-33601: nscd: Daemon may terminate on memory allocation failure • CVE-2024-33602: nscd: Possible memory corruption • Non-maintainer upload by the ELTS Team. • CVE-2024-2961: Out-of-bounds write in iconv ISO-2022-CN-EXT module • Non-maintainer upload by the ELTS Team. • BZ18036 denial of service in fnmatch, similar to CVE-2015-8984 • Non-maintainer upload by the ELTS Team. • Backport much of the test support infrastructure from 2.24. • CVE-2017-12132 dns spoofing via fragmentation • CVE-2017-12133 clntudp_call use after free	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		1000409 CVE-2018-6485 CVE-2018-11236 CVE-2018-1000001 CVE-2019-9169 CVE-2019-25013 CVE-2020-1752 CVE-2020-10029 CVE-2020-27618 CVE-2020-29573 CVE-2021-3326 CVE-2021-3999 CVE-2021-33574 CVE-2021-35942 CVE-2022-23218 CVE-2022-23219	• CVE-2017-15670 glob buffer overflow • CVE-2017-15671 glob memory leak • CVE-2017-15804 glob buffer overflow • CVE-2017-16997 setuid privilege escalation involving RPATH • CVE-2017-1000408 ld.so amplifiable memory leak • CVE-2017-1000409 ld.so buffer overflow • CVE-2018-6485 and CVE-2018-6551 posix_memalign integer overflow • CVE-2018-11236 32bit realpath buffer overflow • CVE-2018-1000001 getcwd could return a relative path • CVE-2019-9169 regex out of bounds read • CVE-2019-25013 oob read in iconv • CVE-2020-1752 use after free in glob • CVE-2020-10029 sinl buffer overflow • CVE-2020-27618 iconv infinite loop • CVE-2020-29573 printf buffer overflow for non-canonical nans • CVE-2021-3326 iconv abort • CVE-2021-3999 oob write for getcwd size 1 • CVE-2021-33574 mq_notify use after free • CVE-2021-35942 wordexp input validation • CVE-2022-23218 svcunix_create buffer overflow • CVE-2022-23219 clnt_create buffer overflow	

Date	Package	CVE(s)	Synopsys	Hardware Version
2024-06-30	libc-bin	CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602 CVE-2024-2961 CVE-2015-8984 CVE-2017-12132 CVE-2017-12133 CVE-2017-15670 CVE-2017-15671 CVE-2017-15804 CVE-2017-16997 CVE-2017-1000408 CVE-2017-1000409 CVE-2018-6485 CVE-2018-11236 CVE-2018-1000001 CVE-2019-9169 CVE-2019-25013 CVE-2020-1752 CVE-2020-	• Non-maintainer upload by the ELTS Team. • CVE-2024-33599: nscd: Stack-based buffer overflow in netgroup cache • CVE-2024-33600: nscd: Null pointer crashes after notfound response • CVE-2024-33601: nscd: Daemon may terminate on memory allocation failure • CVE-2024-33602: nscd: Possible memory corruption • Non-maintainer upload by the ELTS Team. • CVE-2024-2961: Out-of-bounds write in iconv ISO-2022-CN-EXT module • Non-maintainer upload by the ELTS Team. • BZ18036 denial of service in fnmatch, similar to CVE-2015-8984 • Non-maintainer upload by the ELTS Team. • Backport much of the test support infrastructure from 2.24. • CVE-2017-12132 dns spoofing via fragmentation • CVE-2017-12133 clntudp_call use after free • CVE-2017-15670 glob buffer overflow • CVE-2017-15671 glob memory leak • CVE-2017-15804 glob buffer overflow • CVE-2017-16997 setuid privilege escalation involving RPATH • CVE-2017-1000408 ld.so amplifiable memory leak • CVE-2017-1000409 ld.so buffer overflow • CVE-2018-6485 and CVE-2018-6551 posix_memalign integer overflow • CVE-2018-11236 32bit realpath buffer overflow	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		10029 CVE-2020-27618 CVE-2020-29573 CVE-2021-3326 CVE-2021-3999 CVE-2021-33574 CVE-2021-35942 CVE-2022-23218 CVE-2022-23219	• CVE-2018-1000001 getcwd could return a relative path • CVE-2019-9169 regex out of bounds read • CVE-2019-25013 oob read in iconv • CVE-2020-1752 use after free in glob • CVE-2020-10029 sinl buffer overflow • CVE-2020-27618 iconv infinite loop • CVE-2020-29573 printf buffer overflow for non-canonical nans • CVE-2021-3326 iconv abort • CVE-2021-3999 oob write for getcwd size 1 • CVE-2021-33574 mq_notify use after free • CVE-2021-35942 wordexp input validation • CVE-2022-23218 svcunix_create buffer overflow • CVE-2022-23219 clnt_create buffer overflow	
2024-06-30	libc6	CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602 CVE-2024-2961 CVE-2015-8984 CVE-2017-12132 CVE-2017-	• Non-maintainer upload by the ELTS Team. • CVE-2024-33599: nscd: Stack-based buffer overflow in netgroup cache • CVE-2024-33600: nscd: Null pointer crashes after notfound response • CVE-2024-33601: nscd: Daemon may terminate on memory allocation failure • CVE-2024-33602: nscd: Possible memory corruption • Non-maintainer upload by the ELTS Team. • CVE-2024-2961: Out-of-bounds write in iconv ISO-2022-CN-EXT module	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		12133 CVE-2017-15670 CVE-2017-15671 CVE-2017-15804 CVE-2017-16997 CVE-2017-1000408 CVE-2017-1000409 CVE-2018-6485 CVE-2018-11236 CVE-2018-1000001 CVE-2019-9169 CVE-2019-25013 CVE-2020-1752 CVE-2020-10029 CVE-2020-27618 CVE-2020-29573 CVE-2021-3326 CVE-2021-3999 CVE-2021-33574 CVE-2021-35942 CVE-2022-23218 CVE-	• Non-maintainer upload by the ELTS Team. • BZ18036 denial of service in fnmatch, similar to CVE-2015-8984 • Non-maintainer upload by the ELTS Team. • Backport much of the test support infrastructure from 2.24. • CVE-2017-12132 dns spoofing via fragmentation • CVE-2017-12133 clntudp_call use after free • CVE-2017-15670 glob buffer overflow • CVE-2017-15671 glob memory leak • CVE-2017-15804 glob buffer overflow • CVE-2017-16997 setuid privilege escalation involving RPATH • CVE-2017-1000408 ld.so amplifiable memory leak • CVE-2017-1000409 ld.so buffer overflow • CVE-2018-6485 and CVE-2018-6551 posix_memalign integer overflow • CVE-2018-11236 32bit realpath buffer overflow • CVE-2018-1000001 getcwd could return a relative path • CVE-2019-9169 regex out of bounds read • CVE-2019-25013 oob read in iconv • CVE-2020-1752 use after free in glob • CVE-2020-10029 sinl buffer overflow • CVE-2020-27618 iconv infinite loop • CVE-2020-29573 printf buffer overflow for non-canonical nans	

Date	Package	CVE(s)	Synopsys	Hardware Version
		2022-23219	• CVE-2021-3326 iconv abort • CVE-2021-3999 oob write for getcwd size 1 • CVE-2021-33574 mq_notify use after free • CVE-2021-35942 wordexp input validation • CVE-2022-23218 svcunix_create buffer overflow • CVE-2022-23219 clnt_create buffer overflow	
2024-06-30	multiarch-support	CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602 CVE-2024-2961 CVE-2015-8984 CVE-2017-12132 CVE-2017-12133 CVE-2017-15670 CVE-2017-15671 CVE-2017-15804 CVE-2017-16997 CVE-2017-1000408 CVE-2017-1000409 CVE-	• Non-maintainer upload by the ELTS Team. • CVE-2024-33599: nscd: Stack-based buffer overflow in netgroup cache • CVE-2024-33600: nscd: Null pointer crashes after notfound response • CVE-2024-33601: nscd: Daemon may terminate on memory allocation failure • CVE-2024-33602: nscd: Possible memory corruption • Non-maintainer upload by the ELTS Team. • CVE-2024-2961: Out-of-bounds write in iconv ISO-2022-CN-EXT module • Non-maintainer upload by the ELTS Team. • BZ18036 denial of service in fnmatch, similar to CVE-2015-8984 • Non-maintainer upload by the ELTS Team. • Backport much of the test support infrastructure from 2.24. • CVE-2017-12132 dns spoofing via fragmentation • CVE-2017-12133 clntudp_call use after free • CVE-2017-15670 glob buffer overflow	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		2018-6485 CVE-2018-11236 CVE-2018-1000001 CVE-2019-9169 CVE-2019-25013 CVE-2020-1752 CVE-2020-10029 CVE-2020-27618 CVE-2020-29573 CVE-2021-3326 CVE-2021-3999 CVE-2021-33574 CVE-2021-35942 CVE-2022-23218 CVE-2022-23219	• CVE-2017-15671 glob memory leak • CVE-2017-15804 glob buffer overflow • CVE-2017-16997 setuid privilege escalation involving RPATH • CVE-2017-1000408 ld.so amplifiable memory leak • CVE-2017-1000409 ld.so buffer overflow • CVE-2018-6485 and CVE-2018-6551 posix_memalign integer overflow • CVE-2018-11236 32bit realpath buffer overflow • CVE-2018-1000001 getcwd could return a relative path • CVE-2019-9169 regex out of bounds read • CVE-2019-25013 oob read in iconv • CVE-2020-1752 use after free in glob • CVE-2020-10029 sinl buffer overflow • CVE-2020-27618 iconv infinite loop • CVE-2020-29573 printf buffer overflow for non-canonical nans • CVE-2021-3326 iconv abort • CVE-2021-3999 oob write for getcwd size 1 • CVE-2021-33574 mq_notify use after free • CVE-2021-35942 wordexp input validation • CVE-2022-23218 svcunix_create buffer overflow • CVE-2022-23219 clnt_create buffer overflow	

Date	Package	CVE(s)	Synopsys	Hardware Version
2024-08-03	libcurl3	CVE-2024-7264 CVE-2023-38546 CVE-2023-27533 CVE-2023-27535 CVE-2023-27536 CVE-2023-27538 CVE-2022-27774 CVE-2022-27774 CVE-2022-27782 CVE-2022-32221 CVE-2022-35252 CVE-2022-43552 CVE-2022-22576 CVE-2022-27776 CVE-2022-27781 CVE-2022-32208 CVE-2021-22946 CVE-2021-22947 CVE-2021-22898	• Non-maintainer upload by the ELTS team. • Fix CVE-2024-7264: A denial-of-service vulnerability was found in cURL, an easy-to-use client-side URL transfer library. libcurl's ASN1 parser code has the GTime2str() function, used for parsing an ASN.1 Generalized Time field. If given an syntactically incorrect field, the parser might end up crashing but this flaw can also lead to heap contents getting returned to the application when CURLINFO_CERTINFO is used. • Non-maintainer upload by the ELTS team. • CVE-2023-38546: cookie injection • Non-maintainer upload by the ELTS team. • Fix CVE-2023-27533: A vulnerability in input validation exists in curl during communication using the TELNET protocol may allow an attacker to pass on maliciously crafted user name and "telnet options" during server negotiation. The lack of proper input scrubbing allows an attacker to send content or perform option negotiation without the application's intent. This vulnerability could be exploited if an application allows user input, thereby enabling attackers to execute arbitrary code on the system. • Fix CVE-2023-27535: An authentication bypass vulnerability exists in libcurl in the FTP connection reuse feature that can result in wrong credentials being used during subsequent transfers. Previously created connections are kept in a connection pool for reuse if they match the current setup. However, certain FTP settings such as CURLOPT_FTP_ACCOUNT, CURLOPT_FTP_ALTERNATIVE_TO_USER, CURLOPT_FTP_SSL_CCC, and CURLOPT_USE_SSL were not included in the configuration match checks, causing them to match too easily. This could lead to libcurl using the wrong credentials when performing a transfer, potentially allowing unauthorized access to sensitive information. • CVE-2023-27536: An authentication bypass vulnerability exists in libcurl in the connection reuse feature which can reuse previously established connections with incorrect user permissions due to a failure to check for changes in the CURLOPT_GSSAPI_DELEGATION option. This vulnerability affects krb5/kerberos/negotiate/GSSAPI transfers and could potentially result in unauthorized access to sensitive information. The safest option is to not reuse connections if the CURLOPT_GSSAPI_DELEGATION option has been changed. • Fix CVE-2023-27538: An authentication bypass vulnerability exists in libcurl where it reuses a previously established SSH connection despite the fact that an SSH option was modified, which should have prevented reuse. libcurl maintains a pool of previously used connections to reuse them for subsequent transfers if the configurations match. However, two SSH settings were omitted from the configuration check, allowing	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
			them to match easily, potentially leading to the reuse of an inappropriate connection. • Follow up to CVE-2022-27774: The patch included to address this CVE in 7.38.0-4+deb8u24 contained a defect which could result in a segmentation fault and application crash. The patch is corrected in this update. • Non-maintainer upload by the ELTS Team. • CVE-2022-27774: An insufficiently protected credentials vulnerability exists in curl that could allow an attacker to extract credentials when follows HTTP(S) redirects is used with authentication could leak credentials to other services that exist on different protocols or port numbers. • CVE-2022-27782: libcurl would reuse a previously created connection even when a TLS or SSH related option had been changed that should have prohibited reuse. libcurl keeps previously used connections in a connection pool for subsequent transfers to reuse if one of them matches the setup. However, several TLS and SSH settings were left out from the configuration match checks, making them match too easily. • CVE-2022-32221: When doing HTTP(S) transfers, libcurl might erroneously use the read callback (CURLOPT_READFUNCTION) to ask for data to send, even when the CURLOPT_POSTFIELDS option has been set, if the same handle previously was used to issue a PUT request which used that callback. • CVE-2022-35252: When curl is used to retrieve and parse cookies from a HTTP(S) server, it accepts cookies using control codes that when later are sent back to a HTTP server might make the server return 400 responses. Effectively allowing a "sister site" to deny service to all siblings. • CVE-2022-43552: HTTP Proxy deny use-after-free • Non-maintainer upload by the ELTS team. • Fix CVE-2022-22576: An improper authentication vulnerability exists in curl which might allow reuse OAUTH2-authenticated connections without properly making sure that the connection was authenticated with the same credentials as set for this transfer. This affects SASL-enabled protocols: SMPTP(S), IMAP(S), POP3(S) and LDAP(S) (openldap only). • Fix CVE-2022-27776: A insufficiently protected credentials vulnerability in curl might leak authentication or cookie header data on HTTP redirects to the same host but another port number. • Fix CVE-2022-27781: libcurl provides the CURLOPT_CERTINFO option to allow applications to request details to be returned about a server's	

Date	Package	CVE(s)	Synopsys	Hardware Version
			certificate chain. Due to an erroneous function, a malicious server could make libcurl built withNSS get stuck in a never-ending busy-loop when trying to retrieve thatinformation. • Fix CVE-2022-32208: When curl < 7.84.0 does FTP transfers secured by krb5, it handles message verification failures wrongly. This flaw makes it possible for a Man-In-The-Middle attack to go unnoticed and even allows it to inject data to the client. • Non-maintainer upload by the ELTS Team. • CVE-2021-22946 Crafted answers from a server might force clients to not use TLS on connections though TLS was required and expected. • CVE-2021-22947 When using STARTTLS to initiate a TLS connection, the server might send multiple answers before the TLS upgrade and such the client would handle them as being trusted. This could be used by a MITM-attacker to inject fake response data. • Non-maintainer upload by the ELTS team. • CVE-2021-22898: Information disclosure in connection to telnet servers.	
2024-08-03	curl	CVE-2024-7264 CVE-2023-38546 CVE-2023-27533 CVE-2023-27535 CVE-2023-27536 CVE-2023-27538 CVE-2022-27774 CVE-2022-27774 CVE-2022-27782 CVE-2022-32221	• Non-maintainer upload by the ELTS team. • Fix CVE-2024-7264: A denial-of-service vulnerability was found in cURL, an easy-to-use client-side URL transfer library. libcurl's ASN1 parser code has the GTime2str() function, used for parsing an ASN.1 Generalized Time field. If given an syntactically incorrect field, the parser might end up crashing but this flaw can also lead to heap contents getting returned to the application when CURLINFO_CERTINFO is used. • Non-maintainer upload by the ELTS team. • CVE-2023-38546: cookie injection • Non-maintainer upload by the ELTS team. • Fix CVE-2023-27533: A vulnerability in input validation exists in curl during communication using the TELNET protocol may allow an attacker to pass on maliciously crafted user name and "telnet options" during server negotiation. The lack of proper input scrubbing allows an attacker to send content or perform option negotiation without the application's intent. This vulnerability could be exploited if an application allows user input, thereby enabling attackers to execute arbitrary code on the system.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		CVE-2022-35252 CVE-2022-43552 CVE-2022-22576 CVE-2022-27776 CVE-2022-27781 CVE-2022-32208 CVE-2021-22946 CVE-2021-22947 CVE-2021-22898	• Fix CVE-2023-27535: An authentication bypass vulnerability exists in libcurl in the FTP connection reuse feature that can result in wrong credentials being used during subsequent transfers. Previously created connections are kept in a connection pool for reuse if they match the current setup. However, certain FTP settings such as CURLOPT_FTP_ACCOUNT, CURLOPT_FTP_ALTERNATIVE_TO_USER, CURLOPT_FTP_SSL_CCC, and CURLOPT_USE_SSL were not included in the configuration match checks, causing them to match too easily. This could lead to libcurl using the wrong credentials when performing a transfer, potentially allowing unauthorized access to sensitive information. • CVE-2023-27536: An authentication bypass vulnerability exists in libcurl in the connection reuse feature which can reuse previously established connections with incorrect user permissions due to a failure to check for changes in the CURLOPT_GSSAPI_DELEGATION option. This vulnerability affects krb5/kerberos/negotiate/GSSAPI transfers and could potentially result in unauthorized access to sensitive information. The safest option is to not reuse connections if the CURLOPT_GSSAPI_DELEGATION option has been changed. • Fix CVE-2023-27538: An authentication bypass vulnerability exists in libcurl where it reuses a previously established SSH connection despite the fact that an SSH option was modified, which should have prevented reuse. libcurl maintains a pool of previously used connections to reuse them for subsequent transfers if the configurations match. However, two SSH settings were omitted from the configuration check, allowing them to match easily, potentially leading to the reuse of an inappropriate connection. • Follow up to CVE-2022-27774: The patch included to address this CVE in 7.38.0-4+deb8u24 contained a defect which could result in a segmentation fault and application crash. The patch is corrected in this update. • Non-maintainer upload by the ELTS Team. • CVE-2022-27774: An insufficiently protected credentials vulnerability exists in curl that could allow an attacker to extract credentials when follows HTTP(S) redirects is used with authentication could leak credentials to other services that exist on different protocols or port numbers. • CVE-2022-27782: libcurl would reuse a previously created connection even when a TLS or SSH related option had been changed that should have prohibited reuse. libcurl keeps previously used connections in a connection pool for subsequent transfers to reuse if one of them matches the setup. However, several TLS and SSH settings were left out from the configuration match checks, making them match too easily. • CVE-2022-32221: When doing HTTP(S) transfers, libcurl might erroneously use the read callback (CURLOPT_READFUNCTION) to ask for data to send, even when the CURLOPT_POSTFIELDS option has	

Date	Package	CVE(s)	Synopsys	Hardware Version
			been set, if the same handle previously was used to issue a PUT request which used that callback. • CVE-2022-35252: When curl is used to retrieve and parse cookies from a HTTP(S) server, it accepts cookies using control codes that when later are sent back to a HTTP server might make the server return 400 responses. Effectively allowing a "sister site" to deny service to all siblings. • CVE-2022-43552: HTTP Proxy deny use-after-free • Non-maintainer upload by the ELTS team. • Fix CVE-2022-22576: An improper authentication vulnerability exists in curl which might allow reuse OAUTH2-authenticated connections without properly making sure that the connection was authenticated with the same credentials as set for this transfer. This affects SASL-enabled protocols: SMPTP(S), IMAP(S), POP3(S) and LDAP(S) (openldap only). • Fix CVE-2022-27776: A insufficiently protected credentials vulnerability in curl might leak authentication or cookie header data on HTTP redirects to the same host but another port number. • Fix CVE-2022-27781: libcurl provides the CURLOPT_CERTINFO option to allow applications to request details to be returned about a server’s certificate chain. Due to an erroneous function, a malicious server could make libcurl built withNSS get stuck in a never-ending busy-loop when trying to retrieve thatinformation. • Fix CVE-2022-32208: When curl < 7.84.0 does FTP transfers secured by krb5, it handles message verification failures wrongly. This flaw makes it possible for a Man-In-The-Middle attack to go unnoticed and even allows it to inject data to the client. • Non-maintainer upload by the ELTS Team. • CVE-2021-22946 Crafted answers from a server might force clients to not use TLS on connections though TLS was required and expected. • CVE-2021-22947 When using STARTTLS to initiate a TLS connection, the server might send multiple answers before the TLS upgrade and such the client would handle them as being trusted. This could be used by a MITM-attacker to inject fake response data. • Non-maintainer upload by the ELTS team. • CVE-2021-22898: Information disclosure in connection to telnet servers.	

Date	Package	CVE(s)	Synopsys	Hardware Version
2024-08-12	libgdk-pixbuf2.0-0	CVE-2022-48622	• Non-maintainer upload by the ELTS Team. • CVE-2022-48622: ANI file loader memory corruption	M400 M410 R100E R100NA S1600E S100
2024-08-12	libgdk-pixbuf2.0-common	CVE-2022-48622	• Non-maintainer upload by the ELTS Team. • CVE-2022-48622: ANI file loader memory corruption	M400 M410 R100E R100NA S1600E S100
2024-08-14	libsmartcols1	CVE-2024-28085 CVE-2021-37600	• Non-maintainer upload by the Debian ELTS team. • Fix CVE-2024-28085: Escape sequence injection in wall(1). • d/rules: Build with --disable-use-tty-group to avoid installing wall(1) setgid tty. • Re-upload based 2.25.2-6, not 2.26.2-6. • Non-maintainer upload by the Debian ELTS team. ○ CVE-2021-37600: sys-utils/ipcutils: be careful when call calloc() for uint64 nmembs • Remove existing debian/gbp.conf. • Add debian/.gitlab-ci.yml; allow piuparts and lintian failures.	M400 M410 R100E R100NA S1600E S100
2024-08-14	libuuid1	CVE-2024-28085 CVE-2021-37600	• Non-maintainer upload by the Debian ELTS team. • Fix CVE-2024-28085: Escape sequence injection in wall(1). • d/rules: Build with --disable-use-tty-group to avoid installing wall(1) setgid tty. • Re-upload based 2.25.2-6, not 2.26.2-6. • Non-maintainer upload by the Debian ELTS team. ○ CVE-2021-37600: sys-utils/ipcutils: be careful when call calloc() for uint64 nmembs	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
			- Remove existing debian/gbp.conf. - Add debian/.gitlab-ci.yml; allow piuparts and lintian failures.	
2024-08-14	hostapd	CVE-2024-5290 CVE-2023-52160	- Non-maintainer upload by the ELTS Team. - CVE-2024-5290: Only load libraries from trusted path - Non-maintainer upload by the ELTS Team. - Add salsa CI - Fix CVE-2023-52160: The implementation of PEAP in wpa_supplicant allows authentication bypass. For a successful attack, wpa_supplicant must be configured to not verify the network's TLS certificate during Phase 1 authentication, and an eap_peap_decrypt vulnerability can then be abused to skip Phase 2 authentication. This allows an adversary to impersonate Enterprise Wi-Fi networks.	M400 M410 R100E R100NA S1600E S100
2024-08-14	libblkid1	CVE-2024-28085 CVE-2021-37600	- Non-maintainer upload by the Debian ELTS team. - Fix CVE-2024-28085: Escape sequence injection in wall(1). - d/rules: Build with --disable-use-tty-group to avoid installing wall(1) setgid tty. - Re-upload based 2.25.2-6, not 2.26.2-6. - Non-maintainer upload by the Debian ELTS team. ○ CVE-2021-37600: sys-utils/ipcutils: be careful when call calloc() for uint64 nmembs - Remove existing debian/gbp.conf. - Add debian/.gitlab-ci.yml; allow piuparts and lintian failures.	M400 M410 R100E R100NA S1600E S100
2024-08-14	mount	CVE-2024-28085 CVE-2021-37600	- Non-maintainer upload by the Debian ELTS team. - Fix CVE-2024-28085: Escape sequence injection in wall(1).	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
			- d/rules: Build with --disable-use-tty-group to avoid installing wall(1) setgid tty. - Re-upload based 2.25.2-6, not 2.26.2-6. - Non-maintainer upload by the Debian ELTS team. ○ CVE-2021-37600: sys-utils/ipcutils: be careful when call calloc() for uint64 nmembs - Remove existing debian/gbp.conf. - Add debian/.gitlab-ci.yml; allow piuparts and lintian failures.	
2024-08-14	libmount1	CVE-2024-28085 CVE-2021-37600	- Non-maintainer upload by the Debian ELTS team. - Fix CVE-2024-28085: Escape sequence injection in wall(1). - d/rules: Build with --disable-use-tty-group to avoid installing wall(1) setgid tty. - Re-upload based 2.25.2-6, not 2.26.2-6. - Non-maintainer upload by the Debian ELTS team. ○ CVE-2021-37600: sys-utils/ipcutils: be careful when call calloc() for uint64 nmembs - Remove existing debian/gbp.conf. - Add debian/.gitlab-ci.yml; allow piuparts and lintian failures.	M400 M410 R100E R100NA S1600E S100
2024-08-14	util-linux	CVE-2024-28085 CVE-2021-37600	- Non-maintainer upload by the Debian ELTS team. - Fix CVE-2024-28085: Escape sequence injection in wall(1). - d/rules: Build with --disable-use-tty-group to avoid installing wall(1) setgid tty. - Re-upload based 2.25.2-6, not 2.26.2-6. - Non-maintainer upload by the Debian ELTS team.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ CVE-2021-37600: sys-utils/ipcutils: be careful when call calloc() for uint64 nmembs • Remove existing debian/gbp.conf. • Add debian/.gitlab-ci.yml; allow piuparts and lintian failures.	
2024-08-14	bsdutils	CVE-2024-28085 CVE-2021-37600 CVE-2014-9114 CVE-2014-9114 CVE-2007-5191	• Non-maintainer upload by the Debian ELTS team. • Fix CVE-2024-28085: Escape sequence injection in wall(1). • d/rules: Build with --disable-use-tty-group to avoid installing wall(1) setgid tty. • Re-upload based 2.25.2-6, not 2.26.2-6. • Non-maintainer upload by the Debian ELTS team. ○ CVE-2021-37600: sys-utils/ipcutils: be careful when call calloc() for uint64 nmembs • Remove existing debian/gbp.conf. • Add debian/.gitlab-ci.yml; allow piuparts and lintian failures. • Add patch to fix unshare -r regression. ○ Cherry-picked upstream commit 0bf159413bdb9e32486 "unshare: Fix --map-root-user to work on new kernels" Thanks to Kirill Smelkov • Revert "Trigger update of initramfs on upgrades" • Revert "Add Breaks: live-tools (<<4.0~alpha17-1)" ○ No longer needed since dropping the update-initramfs call. • Fix typo in symlink_to_dir and bump prior-version ○ in other words, fix 2.25.2-4.1 upload. • Add Breaks: grml-debootstrap (<< 0.68)	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ previous versions does not work properly with new util-linux which always identifies atleast one label for every partition (PARTUUID) so lets prevent partial upgrades. • Non-maintainer upload. • Add Breaks: live-tools (<<4.0~alpha17-1) • Non-maintainer upload. • Fix unhandled symlink_to_dir conversion for /usr/share/doc/libblkid-dev • Update POT and PO files and clean up .gmo files • Update German translation, thanks to Mario Blättermann • Update Spanish translation, thanks to Antonio Ceballos Roa • Update French translation • Update Ukrainian translation, thanks to Yuri Chornoivan • Update Brazilian Portuguese translation, thanks to Rafael Ferreira • Update Chinese (simplified) translation, thanks to Wylmer Wang • Update Danish translation, thanks to Joe Hansen • Update Finnish translation, thanks to Lauri Nurmi • Update Japanese translation, thanks to Takeshi Hamasaki • Update Russian translation, thanks to Pavel Maryanov • Trivial unfuzzy • Add debian/patches/libblkid-care-about-unsafe-chars-in-cache.patch ○ from upstream git master commit 89e90ae7 "libblkid: care about unsafe chars in cache"	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ This fixes CVE-2014-9114: blkid command injection see https://security-tracker.debian.org/tracker/CVE-2014-9114 Thanks to Salvatore Bonaccorso • libuuid1: add passwd dependency for user migration • Ship fstrim timer/service units as examples only ○ this works around #757891 and #767429 / #760168 • Only ship fstrim service and timer on linux • Imported Upstream version 2.25.2 • Rebase patch queue on top of v2.25.2 ○ This drops the following patches now included upstream: Report-correct-disk-size-on-GNU-kFreeBSD.-Thanks-Tuc.patch remaining-kFreeBSD-hackery-for-building.patch 2.20.1-1.2.patch kFreeBSD-add-hacks-in-ipcrm-to-avoid-FTBFS.patch libmount-only-invoke-loopcxt-on-linux.patch libmount-only-include-context-on-linux.patch build-sys-build-libmount-everywhere.patch build-sys-use-lutil-for-BSD-only.patch libmount-fix-mnt_is_readonly-ifdef.patch flock-zero-timeout-is-valid.patch build-sys-check-for-libtoolize-rather-than-libtool.patch script-may-be-hangs.patch • Ship fstrim service and timer • Add debian/patches/build-sys-check-for-libtoolize-rather-than-libtool.patch ○ Cherry-picked from upstream commit e71b0aadaa20b21e9 "build-sys: check for libtoolize rather than libtool" Thanks to Helmut Grohne for fixing this upstream (and more). • Add debian/patches/script-may-be-hangs.patch ○ Cherry-picked from upstream commit 032228c9af6fbda5177c "script: may be hangs" • Use usermod instead of chsh in postinst user migration • Use a single usermod call in postinst user migration	

Date	Package	CVE(s)	Synopsys	Hardware Version
			● Silence the attempt to stop uuidd before migration ● Pass -std=gnu99 to CC when cross-building. ● Add debian/patches/libmount-fix-mnt_is_readonly-ifdef.patch ○ Cherry-picked from upstream commit 473c5fb86c43eed "libmount: fix mnt_is_readonly() #ifdef" ○ Fixes Hurd build failure. Thanks to Pino Toscano for fixing this upstream! ● hwclock-set: use both systz and hctosys. Thanks to Ben Hutchings for debugging this. ● Add debian/patches/flock-zero-timeout-is-valid.patch ○ Cherry-picked from upstream commit c4604c38b503c8c46e "flock: zero timeout is valid" ● Trigger update of initramfs on upgrades ● hwclock-set: Don't use 'touch' to create stamp file, as it may not be included in an initramfs (Really ● Put uuid-runtime in Section utils. Thanks to Ben Finney for the suggestion ● Cherry-pick upstream commit 8026fa9bc752 "build-sys: use -lutil for BSD only" debian/patches/build-sys-use-lutil-for-BSD-only.patch ● Upload to unstable. ● Make libmount-dev depend on libblkid-dev (LP: #1096581) ● Drop uuid-dev dependency in libmount-dev package ● Drop explicit disabling of pivot_root on non-linux ● Attempt to stop uuidd before usermod in postinst (LP: #1374648) ● Change build-dep to new unified libsystemd-dev	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• hwclock-set: Use stamp file in /run/udev to ensure we set the clock only once if installed in the initramfs • Rename libuuid user to uuidd in libuuidd1 postinst as well • Imported Upstream version 2.25.1 • Drop duplicated BSD-3-clause license text from debian/copyright • Restart uuidd /after/ upgrade. Thanks to Michael Biebl for the suggestion. • Cherry-pick fdisk/bsd test fix from upstream. Thanks to Aurélien Jarno for solving and submitting this upstream • Imported Upstream version 2.25.1~rc1 • Rebase debian patch set on top of 2.25.1~rc1 ○ Drop patches for things fixed in new upstream release: debian/patches/cfdisk-reenable-cursor-when-quitting.patch debian/patches/fdisk-fix-l-device.patch debian/patches/tests-allow-non-inotify-tailf-to-keep-up.patch debian/patches/tests-fix-fdisk-bsd-for-the-two-possible-sectors-off.patch ○ Refresh remaining patches. • Mark libmount context symbols linux-any • Add patches to make libmount build on kfreebsd • Mark libmount1 as to be built everywhere • Install fsck on every architecture • Add NEWS entry about reinstating fsck on kFreeBSD. Disclaimer: I, Andreas Henriksson, will **not** maintain the patches. • Only install linux32/64 manpages on linux-any • Fix uuid-runtime.postinst to skip rmdir when not needed • fdisk-udeb: use dh-exec to skip sfdisk install on sparc	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Mangle installed files on sparc (sfdisk) • Fix sparc install mangling • Use --disable-mountpoint instead of rm • Use dh-exec (>= 0.13) • Install mips,ppc,s390 setarch symlinks and manpages The "Jonno was here" release. • Drop changelog file from the ancient mount source package. • util-linux: Drop all (obsolete) Replaces/Conflicts • Add Replaces/Breaks bash-completion (<< 1:2.1-3). • Multiple cleanups in debian/control. • Minor cleanup of debian/rules. • Use filter, not findstring, for arch matching • Simplify linux-only install file handling • Use debian/*-udeb.install files for udeb packages. • Fix util-linux lintian override. • Minor uuid-runtime.postinst cleanup • Add d/p/cfdisk-reenable-cursor-when-quitting.patch The "big maintainer-script cleanup" release • Drop debian/uuid-runtime.prerm (and related lintian override) ○ dh_installinit will automatically start and stop services as needed. • Drop debian/libuuid1.postinst (user/group addition) • uuid-runtime: improved user/group handling	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ pre-depend on new libuuid1 to make sure no old user handling is present ○ add code to rename existing libuuid user/group to uuidd and set nologin shell and new home directory. ○ switch to adduser instead of opencoding it since uuid-runtime is Priority: optional (as opposed to libuuid1 which is required) and adduser --system should just do the right thing. ○ change user/group addition to add uuidd instead of libuuid. ○ stop making uuidd setuid, not needed and we don't want anyone to be able to kill the daemon (via uuidd -k) for example. • Drop d/p/Use-libuuid-user-group-in-sysvinit-script-systemd-un.patch • util-linux: drop obsolete hwclock handling from maint-scripts • util-linux: drop obsolete update-mime calls • util-linux: drop obsolete 2.17 upgrade warning • util-linux: drop obsolete /etc/default/rcS → /etc/adjtime migration • Reindent/cleanup all maintainer scripts • Drop outdated debian/README.Debian.hwclock • Drop unused debian/rejected-upstream • Drop outdated debian/uuid-dev.README.Debian • Drop diffutils build-dependency • Drop debian/*.dirs • Attempt to avoid dumb term problem in "more: regexp" test • Minor improvements to verbose-tests.patch • Drop renice bash completion for now	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Include dpkg-dev's pkg-info.mk to get package version • Stop creating unused /etc/fstab.d directory • Use proper getty [hurd-any] for Conflicts/Replaces • Add patches cherry-picked from upstream git master ○ debian/patches/tests-allow-non-inotify-tailf-to-keep-up.patch fixes failing testcase on hurd/kfreebsd. ○ debian/patches/fdisk-fix-l-device.patch fixes regression in fdisk listing partition. • Don't ship dmesg bash-completions for now • Add verbose-tests.patch to get more info from tests • Make testsuite non-fatal for now • Add runuser pam configuration from Fedora • Install bash-completion for selected utilities • Prevent dh_installman from messing up rename.ul manpage • Drop misplaced Multi-Arch property on libblkid1-udeb • Set system time directly from hw clock in udev rule • Don't require nfs-common on NFS-rooted system • Fine-tune hwclock.sh init script LSB dependencies • Keep mandatory Required-Stop LSB header in hwclock.sh init script • Revert "Disable tests for now" • Fix binary-arch only builds • Imported Upstream version 2.25	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Rebase patch queue on top of new upstream release + Drop debian/patches for unused and removed mount-deprecated ○ tries-to-umount-proc-when-told-to-umount-some-dir-pr.patch ○ mount-segfault-when-creating-mtab-and-cannot-determi.patch + Update cfdisk.8 patch to modify new manpage file. + Remaining changes are all trivial refreshes. • Update debian/README.source instructions • Fix PPC fdisk/ddisk rename in debian/rules • Stop installing cytune which is no longer available • Use new consolidated systemd configure option • Add util-linux.NEWS entry • Explicitly configure without python for now • Only install i386 and x86_64 binaries on selected architectures • Add new libsmartcols packages • Update libblkid and libmount symbols/shlibs • Drop unused and uninstallable libmount1-udeb • Update debian/copyright for upstream v2.25 • util-linux: Install new terminal-colors.d(5) manpage • Explicitly disable unused utilities • Use correct configure options on non-linux • Add debian/patches/kFreeBSD-add-hacks-in-ipcrm-to-avoid-FTBFS.patch ○ fixes build failure in ipcrm on kFreeBSD	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Skip installing a whole bunch of utils on non-linux • Add WARNING about missing fsck on non-linux to util-linux.NEWS • new branch, with separated patches. • New upstream release • Rebase patches/v2.20.1 branch (commit ad744ecf) on upstream v2.24.2 tag ○ drop patches for issues that has been fixed upstream: [8f1c9b31] "Fix cve-2013-0157: mount discloses information about …" [f08936ba] "sfdisk: fix calculation due to type mismatch (ix86)" [3f051232] "Fix typo in misc-utils/blkid.c" [b9b0ed84] "drop my_dev_t.h, based on 88d52b16ce4df…" (Squashed into man-page-tweaks-cleanup-my_dev_t.h-ancient-stuff.patch) [9ecca8da] "sparc-utils 'sparc64' binary sets ADDR_LIMIT_32BIT. …" [b153d64e] "Fix typo in unshare manpage." [01cfac31] "agetty: don’t use log_err() for non-fatal errors" ○ drop translation updates conflicting with upstream translation updates: [83bc98c2] "Translation updates, various bugs." ○ drop patch for feature deprecated upstream: [23c9f34b] "hash passphrases - debian compatibility" (losetup encryption support dropped, use cryptsetup.) • debian/source/format: switch to 3.0 (quilt) • gbp-pq export patches in quilt format from rebased branch • debian/watch: fix it - use http and xz extension • debian/control: use source:Upstream-Version instead of reinventing it • Switch to dh7 rules and use dh-autoreconf • bsdutils: don’t try to install removed files • Bump debhelper compat to 9 • Update libblkid1 and libmount1 with added symbols	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Documentation files has been moved/renamed ○ also ship all release notes • util-linux-locales: use wildcard to catch all locales • Upstream no longer ships ddate • Drop obsolete --enable-rdev configure switch • Run wrap-and-sort • Add systemd [linux-any] build dependency ○ gets rid of an ugly configure warning • Bump Standards-Version to 3.9.5 • Incorporate NMU changelogs for 2.20.1-5.[678] ○ Their actual changes are all obsoleted by upstream changes. • Install upstream fstab example in mount docs dir • Install debian fstab example in mount again under new name • Add debian/util-linux.NEWS documenting major changes • Install manpages in util-linux package • Use dh_installinit to install hwclock init.d and default files • Install getopt-parse bash and tcsh examples in util-linux docs dir • Let dh_installmime install util-linux mime config • Let dh_installdirs create /etc/fstab.d/ • Split up old debian/rules hacks further • lintian said mount needed ${misc:Depends} dependency	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Add mount/losetup encryption NEWS and recommend cryptsetup • debian/watch: use https url • debian/copyright: update and make machine readable (DEP-5) • Add debian/gbp.conf • Add myself to uploaders, with Adam Conrads blessing. • Point Vcs-* fields to new collab-maint repository • debian/gbp.conf: gbp-pq --no-patch-numbers • Drop Homepage field • Bump shlibs to latest API according to symbols • Fix hwclock.sh to add a final newline in /etc/adjtime • Stop installing extra license files • debian/copyright: Add missing License paragraphs • debian/gbp.conf: Enable pristine-tar • Imported Upstream version 2.24.2 • Add debian/README.source • Improve package descriptions • Improve bsdutils package description • Use simple (ascii) punctuation marks in debian/changelog ○ replaces fancy utf-8 characters in 2.20.1-1.1 and 2.17.2-3.1 • Use ${misc:Pre-Depends} instead of hardcoding multiarch-support • Fix dh_makeshlibs to add udebs in generated shlibs	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Multi-arch -dev packages • Add missing Multi-Arch line to libmount1 package • Put util-linux-locales in section localization • Fix check for systemd in hwclock-set udev script • Fix mismerge in remaining-kFreeBSD-hackery-for-building.patch • Remove /usr/doc/libblkid-dev symlink in postinst/prerm • Add patch to use "libuuid" user/group instead of "uuidd" • Install uuidd sysvinit script and systemd units • Explicitly configure with socket activation enabled • Ship new utilities chcpu, blkdiscard, wdctl, resizepart, lslocks, nsenter, prlimit, utmpdump • Build-depend on libpam0g-dev and ship runuser utility • Ship mkfs.cramfs and fsck.cramfs manpages • Drop obsolete configure switch enable-libmount-mount • Override localstatedir to /run instead of /var • Ship runuser manpage • Add ppc64el to archs where fdisk is renamed ddisk • Attempt to reinstate cross-building support • Disable tests for now ○ Requires network access and prints scary warnings • Fix Multiarch-support-in-util-linux-build.patch ○ Make sure @libexecdir@ gets expanded in pkg-config files	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Non-maintainer upload. • misc-utils/wipefs.c: In --all mode, wipe several times until no further signatures are found. This is required for file systems like VFAT which can be detected in multiple different ways. This is fixed properly in 2.21 (see LP #1012081), but does not backport well, so use this local hack for now. (LP: #1046665, • Non-maintainer upload. • Add arm64/aarch64 support • Non-maintainer upload. • Fix m4 looping in configure.ac's _UTIL_CHECK_SYSCALL. m4_shiftn(2, sequence of two elements) infloops. • mount should not strip MS_REC for --make-r* options. • Non-maintainer upload by the Security Team. • Fix cve-2013-0157: mount discloses information about the existence of folders • Non-maintainer upload. • Rebuild against new eglibc; no source changes. libblkid.a uses the symbol __secure_getenv which is no longer present (it provides secure_getenv). • Non-maintainer upload. • Ship the /var/lib/libuuid/ directory in the package instead of creating it in postinst. • Non-maintainer upload. • Drop the /etc/default/rcS update from postinst. • French, David Prévot. • Vietnamese, Trần Ngọc Quân. • Dutch, Benno Schulenberg.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Polish, Michał Kułach. • Non-maintainer upload. • agetty: don’t use log_err() for non-fatal errors • agetty: Eliminate another log_err() call. • Fix watch file • sfdisk: fix calculation due to type mismatch (ix86) • Make sure we have non-null mount options. • tries to umount /proc when told to umount /some/dir/proc without an /etc/mtab entry. • Deliver {c,}fdisk-udeb on hurd. • Improve handling of the hardware clock ○ Remove redundant hwclockfirst.sh and hwclock.sh. The reason for this redundant script existing (/etc/localtime not being present until after /usr was mounted AFAICT) no longer exists. The hwclock script has been adjusted to run before checkroot. ○ Migrate existing UTC= setting in /etc/default/rcS to UTC/LOCAL in /etc/adjtime. This removes needless duplication of the setting, and prevents the behaviour of hwclock being overridden, and its configuration overwritten every shutdown. ○ The hwclock init scripts now use /etc/adjtime instead of the --utc and --localtime options (based on the UTC setting). ○ Add /etc/default/hwclock and hwclock(5) which permit configuration without editing the initscript, and also document all the undocumented variables used by the scripts. ○ The udev hwclock-set script runs hwclock --tzset unconditionally in all cases (it’s a no-op for UTC). ○ The user running "hwclock --systohc (--utc|--localtime)" is now handled correctly. The clock state is recorded in /etc/adjtime and correctly handled on system restart. This means the UTC setting in /etc/default/rcS doesn’t create problems by requiring	

Date	Package	CVE(s)	Synopsys	Hardware Version
			two separate changes (changing the UTC setting and running hwclock) to do the same thing. ○ Comment out the now-obsolete UTC= setting in /etc/default/rcS, with a reference to /etc/adjtime and hwclock(8). ○ systemd uses /etc/adjtime as for hwclock to store the hardware clock UTC/LOCAL configuration. This change means there’s a single place to store the hardware clock configuration for all init systems. • Polish Debconf Translation. • fix lintian error • Drop broken Pre-Depends: multiarch-support on udeb. • Support /etc/default/hwclock. • fix lintian error • Better english in mount.8. • Multiarch support in util-linux build. • Drop ancient and technically incorrect workaround for hwclock ordering in postinst. • Re-enable ddate, disabled by default upstream in 2.20. • Ack 2.20.1-1.2 • Re-enable ddate. • reenable line. • Deliver the correct upstream changelog. • Fix typo in misc-utils/blkid.c. • fix FTBFS on !linux-any. • Preserve the ACPI wakeup time when updating the hardware clock.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Fix typo in unshare manpage. • Enable hardened build flags. • Non-maintainer upload. • Fixing FTBFS on !linux • Only enable partx where it is supported • Handle vc flags missing on FreeBSD • Fix tty creation on kFreeBSD taking patch from 2.19 • Non-maintainer upload. • Fix FTBFS by running autoreconf -vfi before calling ./configure, which looks better than patching Makefile.in's manually. Thanks to Thorsten Glaser for reporting, and to Simon Ruderich for suggesting a patch • Add autoconf, automake, autopoint, and libtool to Build-Depends accordingly. • Set severity to "high" for the RC bug fix. • New upstream • Various merge fixes [with edits - lamont] ○ drop old unused patches ○ cleanup debian/rules ○ updated symbols files for lib{blkid,mount,uuid}1 • merge in 2.19.1-{3..5} • deliver /etc/fstab.d • add korean debconf pofile. • Add build-arch and build-indep targets.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Conflict/Replace fstrim to provide smooth upgrades • Don’t run hwclock-set when running under systemd • Switch to using linux-any in place of lists • Add missing patch from #631468 to fix agetty linkage on k*bsd • Apply two patches from Michael Biebl <biebl@debian.org>: ○ disable libmount on !linux, fixing kfreebsd FTBFS ○ remove empty /usr/share/locale/ from util-linux • Apply patch from Roger Leigh <rleigh@debian.org> to make hwclock.sh correctly support /run/udev in addition to /dev/.udev • Build with arch:all to resurrect util-linux-locales • Add myself to Uploaders, following a short conversation with LaMont. • deliver findmnt in mount, rather than util-linux • Dutch transations. • Japanese translation. • Finnish debconf templates. • Update with current translations • Enable libmount; new packages libmount1, libmount-udeb and libmount-dev added; bump standards-version • update Indonesian translations. • debconf po file for Catalan. • Add Homepage: to control. • New upstream • NMU	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Bump to Standards-Version 3.9.1. • Drop XS- prefixes on Vcs-Git and Vcs-Browser fields. • Patch from Konstantinos Margaritis to add preliminary armhf support. • Add watch file. • Ack NMU from Christian Perrier <bubulle@debian.org> ○ Fix encoding for Danish and Slovak debconf translations • Brazilian Portuguese debconf templates translation. • fix mangled characters in debconf translations • dh_installdebconf is needed in binary-arch, not so much in -indep. Based on report from Adam D. Barratt <adam@adam-barratt.org.uk>. • nb translations. • Portuguese debconf translations. • Italian translations. • russian debconf translations. • Swedish debconf translations. • Danish translations. • French debconf translations. • German debconf translations. • Spanish debconf translations. • hwclock: [m68k] unbreak FTBFS with recent (>= 2.4.18?) kernels. • Slovak transtions. • Czech debconf translations.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- Merge in all those NMUs that were never pushed to me in bugs. - mount: don’t canonicalize "spec" with --no-canonicalize option. - fdisk: fix freespace boundaries calculation on SGI disklabel. - Deliver agetty as both agetty and getty, preferring agetty. - Declare source format (1.0) - use debconf (iff installed) to warn about noauto fileysstems with non-zero pass numbers. - update lintian-overrides, actually install them in the deb - Non-maintainer upload. - Report correct disk size on GNU/kFreeBSD. Thanks Tuco. - Non-maintainer upload. - Revert the switch from slang2 to ncurses5. There is no udeb for ncurses, so that change broke cfdisk-udeb - Non-maintainer upload. - Apply trivial patch by Adam D. Barratt (thanks!): Only attempt to link locale-specific files in to the cfdisk-udeb hierarchy if cfdisk-udeb is actually being built. - Set urgency to "high" since some packages are waiting for util-linux. - Switch from slang2 to ncurses5. - Merge remote branch 'origin/stable/v2.17' into stable/v2.17 - Restore dropped dep on initscripts. - Add preliminary powerpcspe support. - should build Depend: dpkg or install-info. - pretty up the removal of /usr/share/info/dir	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Fix fallocate configure check. • libblkid: reset BLKID_TINY_DEV flag in blkid_probe_set_device • mount: posix option of vfat is obsolete • mount: update documentation about barrier mount options • sfdisk: confused about disk size • mount: fix typo in mount.8 • fdisk: sleep-after-sync and fsync usage • lscpu: add {32,64}-bit CPU modes detection • tests: refresh lscpu tests • docs: update AUTHORS file • docs: update v2.17 ReleaseNotes • build-sys: release++ (v2.17) • fdisk: don’t include scsi.h • libblkid: restrict RAID/FS proving for small devices (1.4MiB) • libblkid: read() optimization for small devices • tests: fix RAIDs tests • libblkid: call read() per FAT root dir entry • libblkid: set minimal size for jfs, reiser, swap and zfs • libblkid: read whole SB buffer (69kB) on large disks • libblkid: don’t call read() per FAT dir-entry on large disks • libblkid: add minimal sizes for OCFS and GFS	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• tests: update FS test images • libblkid: rewrite blkid_probe_get_buffer() • blkid: probe for PT, don’t probe for FS on small whole-disks • libblkid: add sanity checks for FAT to DOS PT parser • libblkid: don’t probe for GPT and Unixware PT on floppies • login: don’t link PAMed version with libcrypt • libblkid: more robust minix probing • blkid: add newline when only one value is printed • login: check that after tty reopen we still work with a terminal • fdisk: use optimal_io_size • fdisk: use "optimal I/O size" in warnings • wipefs: ignore devices with partition table • libblkid: don’t return error on empty files • fdisk: don’t check alignment_offset against geometry • fdisk: fix check_alignment() • fdisk: cleanup alignment, default to 1MiB offset • fdisk: fix default first sector • fdisk: cleanup warnings • tests: add fdisk alignment tests • tests: fix and update old fdisk tests • mount: warn users that mtab is read-only	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• cal: fix first day of the week calculation on BE systems • build-sys: remove duplicate #includes • blkid: fix #ifdef HAVE_TERMIO[S]_H • build-sys: add missing tests for libuuid and libblkid • mount: advise users to use "modprobe", not "insmod" • include: add min/max macros • fdisk: use more elegant way to count and check alignment • tests: update fdisk tests • fdisk: cleanup help, add -h option • fdisk: fallback for topology values • fdisk: fix ALIGN_UP • fdisk: add -c option (switch off DOS mode) • fdisk: use 1MiB offset and grain always when possible • tests: update fdisk tests • fdisk: don't use 1MiB grain on small devices • blkid: report open() errors in low-level probing • tests: update fdisk tests (add whitespaces) • docs: update AUTHORS file • docs: add v2.17.1 ReleaseNotes • build-sys: release++ (v2.17.1-rc1) • swapon: fix swapsize calculation	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• fdisk: swap VTOC values for warning messages • docs: update AUTHORS file • docs: update v2.17.1 ReleaseNotes • build-sys: release++ (v2.17.1) • docs: fix small typo in v2.17.1-ReleaseNotes • libblkid: support alignment_offset=-1 • libblkid: more robust minix probing • libblkid: fix display of device size • swapon: remove " (deleted)" from filenames from /proc/swaps • libblkid: remove "0x" prefix from DRBD UUID • wipefs: cleanup usage() and man page • mount: more explicitly explain fstab usage in mount.8 • lib: add #ifndef around min() max() macros • fdisk: fix -b <sectorsize> • docs: update AUTHORS file • docs: add v2.17.2 ReleaseNotes • build-sys: release++ (v2.17.2) • po: merge changes • namei: fix man page formatting • cfdisk: set '[Quit]' as default menu item on first run instead of '[Bootable]'. • cfdisk: set '[New]' as default item on menu for non allocated space instead of '[Help]'.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- libblkid: fix ZSF detection - libblkid: DRBD support for blkid - libblkid: fix segfault in drdb - sfdisk: make sure writes make it to disk in write_partitions() - libblkid: disable read-ahead when probing device files - ionice: fix typo - pg: command enters infinite loop - mount: properly ignore comments in /etc/filesystems - new upstream - lintian cleanup - updated symbols file for libblkid1 - drop use of install-info in postinst, uses triggers now - adjust mount.8 manpage to avoid man error - lscpu: fix cpuid opcode detection - login: use fd instead of pathname for update tty's owner and permissions - libblkid: fix infinite loop when probe chain bails out early - po: update id.po (from translationproject.org) (Arif E. Nugroho) - po: update ja.po (from translationproject.org) (Makoto Kato) - po: update cs.po (from translationproject.org) (Petr Pisar) - po: update eu.po (from translationproject.org) (Mikel Olasagasti Uranga) - po: update eu.po (from translationproject.org) (Mikel Olasagasti)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• po: update zh_CN.po (from translationproject.org) (Ray Wang) • po: update pl.po (from translationproject.org) (Jakub Bogusz) • po: update vi.po (from translationproject.org) (Clytie Siddall) • po: update fi.po (from translationproject.org) (Lauri Nurmi) • flock: fix hang when parent ignores SIGCHLD • docs: update TODO list • docs: update AUTHORS file • docs: update v2.17 ReleaseNotes • build-sys: release++ (v2.17-rc2) • lib: bug (typo) in function MD5Final() • docs: add ngettext() into TODO file • docs: update v2.17 ReleaseNotes • build-sys: release++ (v2.17-rc3) • docs: add LGPLv2+ to list of licenses • libblkid: fix Adaptec RAID detection • libblkid: fix highpoint37x detection • libblkid: rename highpoint RAIDs to hpt{37,45}x_raid_member • tests: add adaptec RAID test • tests: add hpt37x RAID test • tests: add hpt45x RAID test • tests: add isw RAID test	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• tests: add jmicron RAID test • tests: add lsi RAID test • tests: add nvidia RAID test • tests: add promise RAID test • tests: add silicon RAID test • mount: disable --no-canonicalize for non-root users • umount: add --no-canonicalize • po: merge changes • po: fix msgid bugs • po: merge changes • po: update pl.po (from translationproject.org) (Jakub Bogusz) • po: update cs.po (from translationproject.org) (Petr Pisar) • po: update eu.po (from translationproject.org) (Mikel Olasagasti Uranga) • New upstream version • hwclockfirst.sh: initscript LSB header in conflict with update-rc.d options. • hwclock*.sh: one more round of header tweaks. • Acknowledge Aurelien Jarno NMU • Non-maintainer upload. • Upload to unstable. • Don’t ship *.la files. • Add avr32 to debian/control	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Remove the outdated debian/shlibs.local file. • Remove the auto-update of symbols files from debian/rules. • Remove symbols from the debian/libuuid1.symbols files which were never part of the public ABI, like uuid_pack/uuid_unpack and were falsely copied over from e2fsprogs. • Strip the Debian revision in the symbols files. • Create a shlibs file for libblkid1 and libuuid1 and bump it to >= 2.16 to ensure correct udeb shlibs dependencies. • Remove *.la files and empty /usr/include and /usr/lib/pkgconfig directories from the util-linux package. • Only check for ENOMEDIUM when ENOMEDIUM is defined. Fixes build on GNU/kFreeBSD. • hwclock: fix mismatched popen/fclose. • ionice: Allow setting the none class • build-sys: fix "make -C" bug • build-sys: fix blkid.h include for old e2fsprogs • blkid: make libuuid optional • build-sys: rename /libs to /shlibs • build-sys: complete /libs to /shlibs rename • blkid: fix "hangs forever with partition type mdraid" • blkid: blkid_do_safeprobe() has to be tolerant to RAIDs • blkid: cleanup debug messages and return codes in blkid_do_probe() • tests: add functions for work withdisk images • mount: fix undefined reference to `security_get_initial_context'. gentoo: #270168	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• libuuid: import UUID library from e2fsprogs • libuuid: add --disable-libuuid and LIBUUID_VERSION • libuuid: add info about u-l-ng to man pages • libblkid: update man page • build-sys: add UTIL_{SET,RESTORE}_FLAGS • build-sys: fix headers in mkswap and libblkid • build-sys: cleanup libuuid stuff • mount: (and fsck) remove libvolume_id support • build-sys: add --disable-libblkid, remove volume_id support • build-sys: enable fsck by default • build-sys: add --disable-tls • uuidgen: new command (from e2fsprogs) • libuuid: add .gitignore • uuidd: new command (UUID daemon from e2fsprogs) • build-sys: add --disable-uuidd • tests: fix 'delete extended partition' checksum • libblkid: fix reiserfs name • tests: add mdraid libblkid test • tests: fix reiserfs test • tests: don’t run some mount tests for non-root users • tests: remove broken Xen dumps for lscpu	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• tests: move lscpu /proc and /sys dumps to tarballs • tests: fix script that creates lscpu dumps • docs: add missing commands/projects to AUTHORS file • mount: use TAG parsing function from libblkid • losetup: add --set-capacity • mount: cleanup notes about -l option in mount.8 • mount: add ext4 to mount.8 • mount: add ext4 to the list of filesystems in mount.8 • mount: use "none" fstype for MS_PROPAGATION mounts • mount: move MS_{PROPAGATION,BIND,MOVE} detection • libblkid: don’t require udev symlinks verification for non-root users • switch_root: new command • build-sys: add --disable-switch_root • switch_root: fix coding style • switch_root: rewrite to use fstatat() and unlinkat() • build-sys: check for openat() and linux for switch_root • switch_root: use err.h, clean up return codes • switch_root: clean up argv[] usage, add -h and -V • switch_root: use snprintf() rather tan str{cpy,cat}() • switch_root: add man page • docs: refresh TODO list	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• docs: remove obsolete information from fstab example. • umount: clean up help output. • mount: add info about obsolete vfat options to mount.8. • losetup: suggest to use modprobe rather than insmod in losetup.8. • mount: a little clean up info about loopdevs in man page. • build-sys: fix libuuid Makefile.am • docs: update AUTHORS file • build-sys: fix --disable-uuidd • docs: add v2.16 ReleaseNotes • docs: update v2.16-ReleaseNotes • build-sys: release++ (v2.16-rc1) • uuidd: move uuidd files from /var/lib/libuuid to /var/run/uuidd • libuuid: move clock state file from /var/lib to /var/run • losetup: fix return codes of functions arounf is_associated() • include: clean up *PATH_DEV** macros • Revert "libuuid: move clock state file from /var/lib to /var/run" • libblkid: fix #ifdefs readability • libuuid: add install-hook for libuuid.[a,so] devel files • libblkid: add install-hook for libuuid.[a,so] devel files • buildsys: move $usr{bin,sbin,lib}execdir definition to ./configure • libblkid: fix $libdir in blkid.pc	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• libuuid: fix $libdir in uuid.pc • docs: remove example.files/rc[.local] • uuidd: move uuidd.rc to misc-utils directory • uuidd: fix $PIDFILE in uuidd.rc • uuidd: init /var/run/uuidd, add option for on-demand mode to .rc file • include: fix _PATH_DEV • raw: undeprecate raw • blkid: move to misc-utils/ directory • docs: update AUTHORS file • docs: update v2.16 ReleaseNotes • build-sys: release++ (v2.16-rc2) • build-sys: fix exec/data install hooks • build-sys: improve symlinks creation in shlibs/ • build-sys: rename to _execdir • libuuid: fix parallel building • build-sys: improve $libdirname definition • libblkid: add stdarg.h to blkidP.h • build-sys: fix libuuid and libblkid version-info • docs: update AUTHORS file • libuuid: generate uuid_generate_{random,time}.3 man page links • docs: update v2.16 ReleaseNotes	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• build-sys: release++ (v2.16) • po: refresh POTFILES.in • po: merge changes • raw: Use the RAW_SETBIND ioctl without stat’ing the raw# file • switch_root: use file descriptor instead of path for recursiveRemove() • switch_root: fork before cleaning up the filesystem. • switch_root: do recursiveRemove after our root is moved to avoid races. • mount: allow loop suid umount. suse: #461732 • build-sys: reverse shlibs installation • switch_root: add subroot support • fdisk: (and cfdisk) fix to be consistent about maximum heads • fdisk: add simple test for doslabel stuff • blkid: fix LVM1 probe • blkid: add device-mapper snapshot cow device probe • mount: when a remount to rw fails, quit and return an error • build-sys: fix typo from 30688dde55f637c9b984809c685b61378b82805f • cal: uClibc has langinfo.h but not _NL_TIME_WEEK_1STDAY. • ldattach: add N_PPS support • lscpu: fix cpuid code on x86/PIC • losetup: handle symlinks in /dev/loop/ • build libblkid binary packages	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• build libuuid binary packages • libuuid: Make sure fd's 0, 1, and 2 are valid before exec'ing uuidd • uuidd: Avoid closing the server socket when calling create_daemon() • libuuid, uuidd: Avoid infinite loop while reading from the socket fd • libuuid: Don't run uuidd if it would fail due to permission problems • po: fix typo in French translation. mandriva: #42783 (Olivier Blin) • po: update fi.po (from translationproject.org) (Lauri Nurmi) • po: update fr.po (from translationproject.org) (Nicolas Provost) • po: update vi.po (from translationproject.org) (Clytie Siddall) • po: update cs.po (from translationproject.org) (Petr Pisar) • chrt: don't assume SCHED_BATCH and SCHED_IDLE exist • remaining kFreeBSD hackery for building. • metafile changes for kFreeBSD buildability hackery. • lscpu: fix cpuid code on x86/PIC • losetup: handle symlinks in /dev/loop/ • Add keybuk as uploader. • meta: cleanup rules targets • hwclock: only call --systz from the udev rule • hwclock: make start a no-op when udev is running • rules: Install udev rules into /lib/udev/rules.d • fdisk: (and cfdisk) fix to be consistent about maximum heads	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- cal: Highlight today even when month or year specified - cal: uClibc has langinfo.h but not _NL_TIME_WEEK_1STDAY. - build-sys: fix "make -C" bug - build-sys: fix blkid.h include for old e2fsprogs - blkid: make libuuid optional - blkid: fix "hangs forever with partition type mdraid" - blkid: blkid_do_safeprobe() has to be tolerant to RAIDs - blkid: cleanup debug messages and return codes in blkid_do_probe() - mount: fix undefined reference to `security_get_initial_context'. gentoo: #270168 - libblkid: update man page - libblkid: fix reiserfs name - build-sys: add UTIL_{SET,RESTORE}_FLAGS - build-sys: fix blkid detection in configure.ac - tests: add mdraid libblkid test - tests: fix reiserfs test - tests: don’t run some mount tests for non-root users - tests: remove broken Xen dumps for lscpu - tests: move lscpu /proc and /sys dumps to tarballs - tests: fix script that creates lscpu dumps - docs: update AUTHORS file - docs: add v2.15.1 ReleaseNotes	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• docs: add missing commands/projects to AUTHORS file • build-sys: release++ (v2.15.1-rc1) • mount: use "none" fstype for MS_PROPAGATION mounts • mount: move MS_{PROPAGATION,BIND,MOVE} detection • docs: update v2.15.1 ReleaseNotes • build-sys: release++ (v2.15.1) • po: merge changes • po: update vi.po (from translationproject.org) (Clytie Siddall) • chrt: don't assume SCHED_BATCH and SCHED_IDLE exist • kFreeBSD hackery for building. • lscpu: fix cpuid code on x86/PIC • losetup: handle symlinks in /dev/loop/ • Add keybuk as uploader. • fdisk: (and cfdisk) fix to be consistent about maximum heads • cal: Highlight today even when month or year specified • cal: uClibc has langinfo.h but not _NL_TIME_WEEK_1STDAY. • build-sys: fix "make -C" bug • build-sys: fix blkid.h include for old e2fsprogs • blkid: make libuuid optional • blkid: fix "hangs forever with partition type mdraid" • blkid: blkid_do_safeprobe() has to be tolerant to RAIDs	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• blkid: cleanup debug messages and return codes in blkid_do_probe() • mount: fix undefined reference to `security_get_initial_context'. gentoo: #270168 • libblkid: update man page • libblkid: fix reiserfs name • build-sys: add UTIL_{SET,RESTORE}_FLAGS • build-sys: fix blkid detection in configure.ac • tests: add mdraid libblkid test • tests: fix reiserfs test • tests: don't run some mount tests for non-root users • tests: remove broken Xen dumps for lscpu • tests: move lscpu /proc and /sys dumps to tarballs • tests: fix script that creates lscpu dumps • docs: update AUTHORS file • docs: add v2.15.1 ReleaseNotes • docs: add missing commands/projects to AUTHORS file • build-sys: release++ (v2.15.1-rc1) • po: merge changes • po: update vi.po (from translationproject.org) (Clytie Siddall) • chrt: add a comment about non POSIX 1003.1b attributes in chrt.1 • agetty: IUCLC and OLCUC are Linux extensions • blkid: remove whole-disk entries from cache when partitions are found	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• docs: add a note about /proc/sys/kernel/random/uuid • ionice: change Jens Axboe’s email • losetup: mount endless loop hang. novell: #449646 • cfdisk: fix "cannot seek on disk drive" bug. • blkid: split SONAME and LIBBLKID_VERSION • blockdev: fix possible buffer overflow • fdisk: fix max. ptname • sfdisk: fix possible buffer overflow • docs: add entry about /proc/partitions parsing • blkid: rename blkid_evaluate_spec to blkid_evaluate_tag • tests: fix -regex in run.sh • blkid: linux_raid - fix logic for volumes with size == 0 • blkid: use /dev/mapper/<name> rather than /dev/dm-<N>. red: #497259 • blkid: use /sys/block/dm-<N>/dm/name • docs: update AUTHORS file • docs: update v2.15 ReleaseNotes • build-sys: release++ (v2.15) • po: merge changes • po: update fr.po (from translationproject.org) (Nicolas Provost) • po: update cs.po (from translationproject.org) (Petr Pisar) • po: update id.po (from translationproject.org) (Arif E. Nugroho)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• lib: do not include <linux/fd.h> in ismounted.c • Package • mount: Add strictatime support • blkid: add ZSF support • blkid: fix exit codes in blkid(8) • hwclock: pass --noadjfile if /etc/adjtime not writable • hwclock: always pass --rtc to hwclock calls • blkid: check idinfo[] index • blkid: add ZSF test • blkid: update TODO • blkid: add TODO note about blkid_evaluate_spec_to_buffer() • blkid: add new requirements to TODO list • login: use open(2) rather then access(2) for $HOME/.hushlogin • docs: update AUTHORS file • blkid: add tst_types.c to Makefile.am • docs: update v2.15 ReleaseNotes • build-sys: release++ (v2.15-rc2) • blkid: rename blkid_debug_init to blkid_init_debug • po: merge changes • fdisk: suggest partprobe(8) and kpartx(8) when BLKRRPART failed • mkfs.cramfs: lower memory requirements for layouts with duplicate files	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• hwclock: omit warning about drift if --noadjfile given • mount: retry on ENOMEDIUM • lscpu: return EXIT_SUCCESS at the end • fdisk: add some missing includes • mkfs.minix: fix size detection • cfdisk: accept yes/no as fallback • losetup: try to set up loop readonly if EACCES • include: move swapheader.h to include • swapon: add swap format detection and pagesize check • Disable the fallback clause in hwclock when /dev/rtc cannot be opened. LP: #274402 • hwclock: unshadow a diagnostic printf • hwclock: delay loop in set_hardware_clock_exact • mount: sundries.h add klibc support • mount: s/MOUNTED/_PATH_MOUNTED/ • disk-utils: s/MOUNTED/_PATH_MOUNTED/ • dmesg: nuke old glibc 5 support • misc-utils: write include signal.h directly • whereis: include dirent.h instead sys/dir.h • disk-utils: include fcntl.h directly (mkfs.cramfs, raw) • fdisk: exit(3) needs stdlib.h include • remove CVS keywords	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• mount: add shortoptions for bind, move and rbind • use getpagesize() • partx: don’t redeclare daddr_t • sfdisk: fix Compilation Error • rtcwake: support not suspending • ionice: Extend the man page to explain the "none" class and cpu-nice inheritance • build-sys: add --disable-mount • dmesg: Add -r (raw) option. • hwclock: remove x86_64-specific bogon • mount: add norealtime to mount.8 • hwclock: always reads hardware clock. • mount: warn on "file_t" selinux context. red: #390691 • selinux: is_selinux_enabled() returns 0, 1 and -1 • umount: improve "-d" option for autoclear loops • losetup: clean up code around LO_FLAGS_AUTOCLEAR • write: doesn’t check for tty group. red: #454252 • build-sys: cleanup sys-utils/Makefile.am • mount: make file_t SELinux warning optional and shorter • mount: add info about tz=UTC option for FAT to mount.8 • losetup: looplist_* refactoring, remove scandir() • rtcwake: cleanup return codes	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• hwclock: cleanup help output and man page • mount: add docs about utf8=0 for vfat. red: #454354 • hwclock: use carefully synchronize_to_clock_tick() return codes • hwclock: use time limit for synchronization busy wait • hwclock: read_hardware_clock_rtc() need to return error codes • scriptreplay: new implementation is out-of-sync • ionice: cleanup man page • ionice: cleanup error messages, add NLS support • docs: TODO update • tests: detect libvolume_id when mount(8) is compiled • fdisk: remove obsolete information from man page • hwclock: don’t open /dev/rtc repeatedly • swapon: -a has to complain, fix leaks • fdisk: warn users about 2.2TB dos partition limit • fdisk: don’t check for GPT when asked for disk size only • fdisk: round reported sizes rather than truncate • losetup: remove dependence on minor numbers • login: fix warning "dereferencing type-punned pointer will break strict-aliasing rules" • ionice: add strtol() checks, cleanup usage text and man page • ipcmk: fix error codes and error messages • ipcmk: add NLS support	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• build-sys: add -luuid to BLKID_LIBS • chrt: add NLS support, clean error messages and return codes • mount: fix typo • mount: add info about /proc/mounts to mount.1 • fsck.cramfs: fix compiler warning • login: fix compiler warning (int32 time() arg) • losetup: missing EBUSY error hint message • mount: mtab created multiple times with -a option • mount: remove link to namesys.com • mount: sync FAT info in mount.8 with Documentation/filesystems/vfat.txt • mount: sync tmpfs info in mount.8 with Documentation/filesystems/tmpfs.txt. red: #465761 • ipcs: fix exit codes, remove tailing white-spaces. red: #465911 • hwclock: remove "cli" and "sti" from i386 CMOS code • docs: update TODO list • lscpu: add Hypervisor detection • tests: add mk-lscpu-input.sh • tests: add lscpu(1) test for paravirt. Xen i386 • tests: add lscpu(1) test for fullvirt. Xen x86_64 • tests: refresh Makefile.am (add missing lscpu tests) • fdisk: cannot create partition with starting beyond 1 TB • fdisk: read /proc/partitions in more robust way	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• fdisk: support +cylinder notation • namei: new re-written version • namei: add --owners and --long options • losetup: add warning about read-only mode • build-sys: move pivot_root(8) to sys-utils • pivot_root: clean up • tests: update namei reg.test • fdisk: fix man page typo • tools: add checkincludes.pl (from linux kernel) • tools: rename codecheck-config to checkconfig.sh • tools: add checkconfig to top-level Makefile • fdisk: rename ENABLE_CMDTAGQ macro • getopt: remove unnecessary ifdefs • hwclock: clock.h is included more than once • agetty: sys/types.h and time.h are included more than once • login: cleanup includes • rdev: cleanup includes • tailf: unistd.h is included more than once • mount: add i_version support • mount: reorder list of options in mount.8 • mount: create separate section for fs-independent options in mount.8	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• mount: use subsections in mount.8 DESCRIPTION • docs: add feature-requests from RH bugzilla to TODO list • setterm: fix -blank man page • build-sys: add missing AC_C_BIGENDIAN • mkfs.minix: (and fsck) rename bitops.h • include: swapheader.h is missing in Makefile.am • tests: add swabN() regression test • tests: add MD5 regression test • lib: add __BYTE_ORDER to md5.c • include: use __BYTE_ORDER rather than AC specific WORDS_BIGENDIAN • tests: add md5 regression test • mount: fix mount_static_LDADD • Revert "login-utils: several strings without gettext calls" • TODO: add request to use nl_langinfo() • chfn: several strings without gettext calls • simpleinit: cleanup gettext calls, use snprintf() • refresh gitignore • pg: add gettext call for the help string • fdisk: remove unnecessary gettext call • mount: clean up SPEC canonicalization • mount: add rootcontext= SELinux mount option	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• raw: default to /dev/raw/rawctl • namei: fix buffer overflow • mount: add info about semantics of read-only mount to mount.8 • mount: suggest to use blockdev --setro rather than losetup • mount: finalize support of quoted LABELs/UUIDs • umount: cleanup gefs_by_specdir() • ionice: a little cleanup of "none" description • namei: don't duplicate '/' directory • rtcwake: explain supported modes in rtcwake.8 • namei: add --vertical option • namei: add missing options to namei.1 • rtcwake: add mising .RE to the man page • mount: fix typo in volume_id code • ionice: fix typo in manpage • chrt: output buglet when reporting scheduling class • fdisk: add 0xaf HFS / HFS partition type • mount: non-setuid (POSIX file capabilities) support • tests: check also for /dev/loop/X • fsck.cramfs: segfault with INCLUDE_FS_TESTS and no -x option • docs: add suggestion about TZ=UTC to TODO file • mkfs.minix: add regression test	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• fsck.minix: add regression test • mkfs.minix: remove local implementation of {set,clr}bit • agetty: check for termios.c_line struct member by autoconf • fdisk: cleanup *PATH_DEV** macros • blkid: create basic directories • build-sys: define libdir • blkid: add basic configure.ac stuff and blkid.pc • blkid: merge libblkid code from e2fsprogs/lib/blkid • blkid: minor changes to library build system • blkid: add low level probing API • blkid: add adaptec raid • blkid: optimize for string UUIDs • blkid: add DDF raid • blkid: add ISW raid • blkid: add JMicron RAID • blkid: LSI MegaRAID • blkid: NVIDIA raid • blkid: Promise raid • blkid: add Silicon Image Medlay RAID • blkid: add VIA RAID • blkid: update gitignore	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• blkid: add Linux RAID • blkid: blkdev size fallback • blkid: correctly initialize magics[] arrays • blkid: add ext{2,3,4,4devel} support • blkid: add jfs • blkid: add blkid_probe_get_sb() macro • blkid: add xfs • blkid: fix ext2 SEC_TYPE • blkid: fix xfs label • blkid: add GFS and GFS2 • blkid: add romfs • blkid: add ocfs and oracleasm • blkid: add *attribute* format • blkid: fix blkid_probe_sprintf_version() usage • add reiser and reiser4 • blkid: add HFS and HFS+ • blkid: add GFS2 UUID support • blkid: add HTFS • blkid: add missing hfs.c • blkid: add iso9600 • blkid: add LVM2 support and a fix _sprintf_uuid() bug	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• blkid: add UDF support • blkid: add VFAT support • blkid: re-order list of filesystems • blkid: add LUKS support • blkid: support detection of multiple signatures • blkid: add version and probe FSInfo • blkid: add highpoint{37x,45x} RAIDs • blkid: add lvm1 • blkid: add vxfs • blkid: add minix • blkid: add UFS • blkid: remove unused stuff from Makefile • blkid: add proper copying info • blkid: add TODO file • blkid: add HPFS • blkid: cleanup starts of probing files • blkid: fix highpoint37x offset • blkid: use posix uint32_t in ocfs superblock • blkid: use posix uintXX_t in lvm code • blkid: fix hedeader in ntfs.c • blkid: remove blkid_types.h	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• blkid: add squashfs • blkid: add netware (NSS) • blkid: add sysv and xenix • build-sys: remove use of devmapper library • blkid: use Requires.private and fix the include directory • blkid: fix file descriptor leak when checking for a module • blkid: remove unnecessary ifdef __cplusplus • blkid: add btrfs support • blkid: add DEBUG_LOWPROBE, cleanup a little debug stuff • blkid: add -p and low-probe mode to blkid binary • blkid: add udev string encoding routines • blkid: add udev ID_FS_* output to blkid binary • blkid: refresh TODO file • blkid: use sizeof() for hfs uuid • blkid: refresh TODO file • tests: create subdirs for test scripts • tests: remove input directory • tests: create expected/$(component)/$(testname) • tests: add support for subdirs to basic test functions • tests: add ./run.sh <component> • tests: fix TS_* paths	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• tests: cleanup ts/cal scripts • tests: cleanup ts/col scripts • tests: cleanup ts/hwclock • tests: cleanup ts/ipcs • tests: cleanup ts/login • tests: cleanup ts/look • tests: cleanup ts/namei • tests: cleanup ts/paths • tests: cleanup ts/script • tests: cleanup ts/swapon • tests: cleanup ts/mount • tests: fix output string • tests: add "byte-order" to helpers/test_sysinfo • tests: move some generic stuff from ts_init() to a new ts_init_env() • tests: add support for subtests • tests: fix the final message for subtests • tests: add libblkid regression tests (images from e2fsprogs) • blkid: add a note to TODO list • blkid: fix blkid_safe_string() • tests: remove unexpected exit from *_subtest functions • blkid: fix udev output	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- blkid: add hpfs regression test - blkid: netware SB has to be packed - blkid: add netware regression test - blkid: set size for non-blkdevs, add blkid_probe_strcpy_uuid() - blkid: improve ddf detection - blkid: use blkid_probe_strcpy_uuid() for luks - blkid: remove unnecessary debug message - blkid: fix blkid_do_probe() - blkid: add ddf raid regression test - blkid: fix …_strncpy_uuid - blkid: add ocfs2 version - blkid: add to reiser - blkid: add vol_id call to blkid regression test - blkid: add reg.tests for HFS and HFS+ - blkid: add uuid and version support to gfs2 - blkid: add GFS2 reg. test - blkid: add version support to LVM2 - blkid: add lvm2 reg.test - blkid: add blkid_do_safeprobe() - blkid: cleanup _LOGPROBE debug messages - tests: fix typo in low-probe test	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- blkid: refresh TODO file - blkid: add new options to blkid.8 and help output - blkid: add support for /etc/blkid.conf file - blkid: compile TEST_PROGRAMs - blkid: fix typo (syntax error) - mount: move realpath.c code to lib/ - blkid: add blkid_evaluate_spec() - blkid: clean up man pages - blkid: refresh TODO file - blkid: add findfs(8) - build-sys: add --with=fsprobe=builtin - blkid: start to use ABI versioning - build-sys: libtoolize by libtool-2 - build-sys: libtoolize mount/Makefile.am - build-sys: add temporary libtool *.m4 stuff - blkid: refresh TODO file - blkid: add Christoph's note about libdisk to TODO - mount: generic blkid/volume_id wrapper, use blkid_evaluate_* - build-sys: use pkg-config for blkid and volume_id - blkid: add TODO hint about DM devnames in sysfs - blkid: check calloc() return value	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• blkid: add cmdline interface for blkid_probe_filter_usage() • blkid: add TODO hint about blkid_parse_tag_string() • blkid: fix low-probe mode return codes • fsck: move fsck from e2fsprogs to util-linux-ng • lib: make open_device() optional in fsprobe.c • fsck: link with generic fsprobe wrapper • fsck: cosmetic changes (NLS, paths, …) • lib: add test_ismounted for regression test • tests: add fsck:ismounted reg.test • tests: cleanup ts/bitops • tests: cleanup ts/cramfs/fsck-endianness • tests: cleanup ts/cramfs/mkfs-endianness • tests: cleanup lscpu reg.tests • build-sys: add fsck binary to .gitignore • tests: cleanup ts/minix • tests: cleanup ts/md5 • tests: chmod -x ts/lscpu/mk-input.sh • tests: we needn’t blkid.sh • tests: refresh cal(1) expected outputs • tests: refresh ipcs expected outputs • blkid: blkid_evaluate_spec() shouldn’t ignore $BLKID_FILE	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• mount: inform about UID and eUID when verbose > 2 • tests: disable suid mount test • tests: refresh expected mount(8) outputs • losetup: detach more devices by "-d <loop> [<loop> ..]" • losetup: cleanup man page • tests: remove obsolete stuff from Makefile.am • fsck: remove \007 from warning message • build-sys: add missing files to include/Makefile.am • blkid: fix a syntax nit • fsck: remove useless if-before-free tests • getopt: remove useless if-before-free tests • mount: remove useless if-before-free tests • fdisk: use real sector size in verify() and warn_cylinders() • blockdev: add note that the StartSec is in 512-byte sectors • addpart: 512-byte sectors in code, bytes in man-page • partx: convert hard sector size to 512-byte sectors • partx: don’t duplicate lib/blkdev.c code • fdisk: (and partx) remove BLKGETLASTSECT • partx: use ioctls from lib/blkdev.c • docs: add a note about kpartx to TODO • swapon: do_swapon() refactoring (move stat() checks)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• swapon: add generic swap_get_header() • swapon: simplify spec to devname conversion • swapon: use err.h stuff • swapon: do_swapon() refactoring (split into two functions) • swapon: rewrite SWSUSPEND signature rather than exec mkswap • swapon: cleanup man page • swapon: add -f/--fixpgsz option • simmpleinit: fix gcc warning (buffer size in read()) • mount: fix gcc warning (variable used uninitialized) • blkid: use "char **" rather than "unsigned char** " • blkid: fix gcc warning in blkid_get_cache_filename() • lib: gcc warning in fix fsprobe • lib: fix fsprobe wrapper (const char * is nonsense) • swapon: fix wording in man page • swapon: fix typo s/warn/warnx/ • swapon: add error messages for lseek and write • login: remove "switching users" nonsense from man page • fdisk: support "-b 4096" option • blkid: blkid.static make target • build-sys: cleanup --with-fsprobe help string • renice: add -n option for compatibility with POSIX	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• cal: remove gcc-ism from nl_langinfo() call • flockc: segfaults when file name is not given. red: #489672 • flock: fix printf format error in usage() • flock: add NLS support, remove tailing white-spaces • lib: add is_whole_disk() from fdisk code • mkswap: remove v0 swap space support • lib: add pttype.c for PT types detection • include: add missing files to Makefile.am • lib: pttype: add BSD subpartitions support • lib: pttype: fix DOS detection • lib: pttype - extend the API to work with file descriptors • lib: wholedisk - extend API, add test program • libs: pttype - fix typo • mkswap: zap bootbits • mkswap: clean up man page • blkid: fix non-udev low-probe mode output • lib: fsprobe - fix gcc warning • tests: disable blkid tests when blkid(8) is not compiled • blkid: add missing blkidP.h to Makefile.am • build-sys: refresh generated libtool-2 stuff • include: bitops - explicitly include endian.h	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• build-sys: add $usrlibexecdir and fix paths for [/usr]/lib64 • blkid: fix ocfs2 detection • login: use "remote" as a PAM service name for "login -h" • tests: fix file name is too long (max 99) - gtar • tests: fix typo in lscpu test • docs: update AUTHORS file • docs: update v2.15 ReleaseNotes • build-sys: fix bugs detected by "make distcheck" • build-sys: release++ (v2.15-rc1) • docs: fix typo, cal(8) -→ cal(1) • po: update list of .c files • po: merge changes • po: update POTFILES.in • po: rewrite update-potfiles script • elvtune: add NLS support • fsck.cramfs: add NLS support • mkfs.cramfs: several strings without gettext calls • raw: add NLS support • fdisk: several strings without gettext calls • hwclock: several strings without gettext calls • login-utils: several strings without gettext calls	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• logger: several strings without gettext calls • losetup: several strings without gettext strings • readprofile: several strings without gettext calls • pg: several strings without gettext calls • more: minor fixes to magic() • mount: document newinstance and ptmxmode options to devpts • hwclock: add --systz option to set system clock from itself • debian/control: Add build-dependency on pkg-config • umount: check for overlaid mounts • mount: fix typo • ipcmk: new command • Fix dmesg.1 installation • flock: Allow lock directory • blkis: fix detection of ext4dev as ext4 • blkid: recognize ext3 with test_fs set as ext3 • fdisk: doesn’t handle large (4KiB) sectors properly • blkid: recognize ext4(dev) without journal • blkid: vfat - fix declaration • blkid: hfs - use proper native UUID format • blkid: hfs - do not set UUID for emtpy finder info • lscpu: new command	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• lscpu: --sysroot option and stable cache output • lscpu: regression tests • ionice: let -p handle multiple PIDs • blkid: don’t dereference NULL upon slashless module dependency line • blkid: remove useless if-before-free tests • mount: cleans up mount(8) troff markup • tests: clean up the testing scripts • tests: remove useless return value checks in testing scripts • blkid: support via raid version 2 • mkfs.cramfs: add endianness support to cramfs tools • chrt: support CFS SCHED_IDLE priority and document it • mkswap: non-linux support • fdisk: don’t use get_linux_version() for non-linux • lib: blkdev.c clean up, non-linux support • fdisk: non-linux support (BLK* and HDIO_*) • disk-utils: clean up code, use blkdev_* functions • ldattach: don’t compile for non-linux systems • ipcs: ungettextize the spacing of the table headers • ipcs: adjust some field positions and widths for correct alignment • po: update nl.po (from translationproject.org) • sfdisk: print version should end with a newline	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• build-sys: tgets is not in ncurses but in tinfo • rtcwake: prefer RTC_WKALM_SET over RTC_ALM_SET • more: dont use a.out.h • mount: remove spurious newline from mount.8 • ionice: add -t option. red: #443842 • blkid: Optimize devicemapper support • blkid: Unexport the private symbol blkid_devdirs • blkid: Give a priority bonus to "leaf" devicemapper devices • blkid: Refuse to create a device structure for a non-existent device. • blkid: add fallback to ext4 for 2.6.29+ kernels if ext2 is not present • umount: no checking mount point removal • mkswap: handle 2^32 pages • script: don’t flush input when starting script • tests: refresh and cleanup cramfs/mkfs • blkid: add -L -U options (evaluation API) • cal: determine the first day of week from the locale • po: update id.po (from translationproject.org) (Arif E. Nugroho) • po: update ja.po (from translationproject.org) (Makoto Kato) • po: update cs.po (from translationproject.org) (Petr Pisar) • po: add zh_CN.po (from translationproject.org) (Ray Wang) • po: update fr.po (from translationproject.org) (Nicolas Provost)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• po: update vi.po (from translationproject.org) (Clytie Siddall) • po: update fi.po (from translationproject.org) (Lauri Nurmi) • mount: segfault when creating mtab and cannot determine fsname. • hwclockfirst.sh: use correct LSB header info. • chrt: output buglet when reporting scheduling class • mount: fix typo in volume_id code • docs: update AUTHORS file • docs: update v2.14.2 ReleaseNotes • build-sys: release++ (v2.14.2) • po: merge changes • po: update vi.po (from translationproject.org) (Clytie Siddall) • po: update cs.po (from translationproject.org) (Petr Pisar) • po: update ja.po (from translationproject.org) (Makoto Kato) • po: update nl.po (from translationproject.org) (Benno Schulenberg) • hwclock: omit warning about drift if --noadjfile given • cfdisk: accept yes/no as fallback • fdisk: add some missing includes • losetup: try to set up loop readonly if EACCES • mkfs.minix: fix size detection • mount: retry on ENOMEDIUM • hwclock: unshadow a diagnostic printf	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- mount: sundries.h add klibc support - use getpagesize() - ionice: Extend the man page to explain the "none" class and cpu-nice inheritance - hwclock: remove x86_64-specific bogon - mount: add norealtime to mount.8 - selinux: is_selinux_enabled() returns 0, 1 and -1 - umount: improve "-d" option for autoclear loops - write: doesn’t check for tty group - rtcwake: cleanup return codes - mount: add info about tz=UTC option for FAT to mount.8 - build-sys: cleanup sys-utils/Makefile.am - build-sys: fix dmesg.1 installation - mount: add fallback for versionsort() - mount: add docs about utf8=0 for vfat - scriptreplay: new implementation is out-of-sync - docs: update AUTHORS file - docs: update v2.14.1 ReleaseNotes - build-sys: release++ (v2.14.1-rc1) - losetup: remove unnecessary minor number check - fdisk: don’t check for GPT when asked for disk size only - docs: update AUTHORS file	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• docs: update v2.14.1 ReleaseNotes • build-sys: release++ (v2.14.1-rc2) • docs: update v2.14.1 ReleaseNotes • build-sys: release++ (v2.14.1) • mount: mtab created multiple times with -a option • build-sys: add -luuid to BLKID_LIBS • lib: add __BYTE_ORDER to md5.c • include: use __BYTE_ORDER rather than AC specific WORDS_BIGENDIAN • fdisk: cannot create partition with starting beyond 1 TB • fdisk: remove obsolete information from man page • fdisk: fix man page typo • fdisk: support +cylinder notation • hwclock: remove "cli" and "sti" from i386 CMOS code • login: fix warning "dereferencing type-punned pointer will break strict-aliasing rules" • login: fix compiler warning (int32 time() arg) • losetup: add warning about read-only mode • losetup: missing EBUSY error hint message • mount: add info about /proc/mounts to mount.1 • mount: add i_version support • mount: reorder list of options in mount.8	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• mount: sync FAT info in mount.8 with Documentation/filesystems/vfat.txt • mount: sync tmpfs info in mount.8 with Documentation/filesystems/tmpfs.txt • mount: remove link to namesys.com • mount: create separate section for fs-independent options in mount.8 • mount: fix typo • mount: use subsections in mount.8 DESCRIPTION • mount: warn on "file_t" selinux context • mount: make file_t SELinux warning optional and shorter • setterm: fix -blank man page • mount: fix mount_static_LDADD • fdisk: remove unnecessary gettext call • refresh gitignore • docs: update AUTHORS file • mount: clean up SPEC canonicalization • mount: add rootcontext= SELinux mount option • docs: update v2.14.2 ReleaseNotes • build-sys: release++ (v2.14.2-rc1) • mount: add info about semantics of read-only mount to mount.8 • mount: suggest to use blockdev --setro rather than losetup • mount: finalize support of quoted LABELs/UUIDs • ionice: a little cleanup of "none" description	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• docs: update AUTHORS file • docs: update v2.14.2 ReleaseNotes • build-sys: release++ (v2.14.2-rc2) • po: merge changes • fdisk: several strings without gettext calls • logger: several strings without gettext calls • losetup: several strings without gettext strings • mkfs.cramfs: several strings without gettext calls • readprofile: several strings without gettext calls • mount: cleans up mount(8) troff markup • mount: fix typo • build-sys: tgets is not in ncurses but in tinfo • rtcwake: prefer RTC_WKALM_SET over RTC_ALM_SET • chrt: support CFS SCHED_IDLE priority and document it • ldattach: don’t compile for non-linux systems • ipcs: ungettextize the spacing of the table headers • po: update nl.po (from translationproject.org) • sfdisk: print version should end with a newline • more: dont use a.out.h • mount: remove spurious newline from mount.8 • more: minor fixes to magic()	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• po: update id.po (from translationproject.org) (Arif E. Nugroho) • po: update pt_BR.po (from translationproject.org) (Rodrigo Stulzer Lopes) • po: update zh_CN.po (from translationproject.org) (Ray Wang) • po: add zh_CN.po (from translationproject.org) (Ray Wang) • po: update sv.po (from translationproject.org) (Daniel Nylander) • po: update fr.po (from translationproject.org) (Nicolas Provost) • po: update vi.po (from translationproject.org) (Clytie Siddall) • po: update cs.po (from translationproject.org) (Petr Pisar) • po: update fi.po (from translationproject.org) (Lauri Nurmi) • rules: drop separate configure target. • ddate: 11th, 12th and 13th of month • rtcwake: fix the default mode to "standby" • mount: fix a small typo in mount.8 • Update menu-item number for Debian Installer components. • docs: update AUTHORS file • docs: update v2.14 ReleaseNotes • build-sys: release++ (v2.14) • po: merge changes • po: update hu.po (from translationproject.org) (Gabor Kelemen) • lomount: initialize sizelimit (lost in merge). LP: #230974 • meta: fix description of bsdutils.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• control: add support for sh4. • docs: we already rewrote the scriptreplay script; remove that TODO entry • setarch: add fallback for linux/personality • fdisk: doesn’t recognize the VMware ESX partitions • build-sys: add support ionice for Super-H architecture • mount: remount doesn’t care about loop= • po: merge changes ○ po: update cs.po (from translationproject.org) (Petr Pisar) ○ po: update nl.po (from translationproject.org) (Benno Schulenberg) ○ po: update it.po (from translationproject.org) (Marco Colombo) ○ po: update vi.po (from translationproject.org) (Clytie Siddall) • docs: update 2.14 ReleaseNotes • build-sys: release++ • login: audit log injection attack via login • po: merge changes ○ po: update it.po (from translationproject.org) (Marco Colombo) ○ po: update nl.po (from translationproject.org) (Benno Schulenberg) • ionice: update man page to reflect IDLE class change in 2.6.25 • scriptreplay: gettextize a forgotten messages	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• docs: update v2.14 ReleaseNotes • build-sys: release++ • New upstream version • control: drop -1 version from libslang2-dev build-dep • control: standards-version 3.7.3.0 • login: audit log injection attack via login • po: merge changes ○ po: update it.po (from translationproject.org) (Marco Colombo) ○ po: update nl.po (from translationproject.org) (Benno Schulenberg) • docs: add v2.13.1.1 ReleaseNotes • build-sys: release++ (2.13.1.1) • control: drop -1 version from libslang2-dev build-dep • control: standards-version 3.7.3.0 • Switch to upstream's more-correct fix for LP#206113 • mkswap: when writing the signature page, handle EINTR returns. LP: #206113 • meta: Drop bashism in preinst. • mkswap: when writing the signature page, handle EINTR returns. LP: #206113 • swapon: Reinitialize software suspend areas to avoid future corruption. LP: #66637 • Add menu item numbers for *fdisk udebs. • agetty: make username-in-uppercase feature optional (off by default.).	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• debian/rules: allow cross-building. • hwclock.sh: fix typo. LP: #103680 • mkswap: Set UUID for swap space. • mkswap: -U UUID cleanup • New Upstream Release [Karel Zak] ○ docs: update AUTHORS file ○ docs: update ReleseNotes ○ build-sys: release++ (2.13.1) ○ po: merge files ○ po: update uk.po (from translationproject.org) (Maxim V. Dziumanenko) ○ po: update it.po (from translationproject.org) (Marco Colombo) ○ po: update sl.po (from translationproject.org) (Simon Mihevc) ○ po: update ru.po (from translationproject.org) (Pavel Maryanov) ○ po: update cs.po (from translationproject.org) (Petr Pisar) ○ po: update pt_BR.po (from translationproject.org) (Rodrigo Stulzer Lopes) ○ po: update id.po (from translationproject.org) (Arif E. Nugroho) ○ po: update es.po (from translationproject.org) (Santiago Vila Doncel) ○ po: update hu.po (from translationproject.org) (Gabor Kelemen) ○ po: update eu.po (from translationproject.org) (Mikel Olasagasti)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ po: update ca.po (from translationproject.org) (Josep Puigdemont) ○ po: update sv.po (from translationproject.org) (Daniel Nylander) ○ po: update fr.po (from translationproject.org) (Michel Robitaille) ○ po: update tr.po (from translationproject.org) (Nilgün Belma Bugüner) ○ po: update ja.po (from translationproject.org) (Daisuke Yamashita) ○ po: update nl.po (from translationproject.org) (Benno Schulenberg) ○ po: update pl.po (from translationproject.org) (Andrzej Krzysztofowicz) ○ po: update da.po (from translationproject.org) (Claus Hindsgaul) ○ po: update vi.po (from translationproject.org) (Clytie Siddall) ○ po: update et.po (from translationproject.org) (Meelis Roos) ○ po: update de.po (from translationproject.org) (Michael Piefel) ○ po: update fi.po (from translationproject.org) (Lauri Nurmi) • hwclockfirst.sh: yet more tweaks for LSB init. • meta: mount should pre-depend on its libs • hwclock.sh: add full path to comment. • renice: correctly detect errors in arguments. • docs: update AUTHORS file, add all translators • docs: update ReleaseNotes	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• po: update po files ○ po: update uk.po [Maxim V. Dziumanenko] ○ po: update id.po [Arif E. Nugroho] ○ po: update es.po [Santiago Vila Doncel] ○ po: update hu.po [Gabor Kelemen] ○ po: update it.po [Marco Colombo] ○ po: update sl.po [Simon Mihevc] ○ po: update ru.po [Pavel Maryanov] ○ po: update cs.po [Petr Pisar] ○ po: update pt_BR.po [Rodrigo Stulzer Lopes] ○ po: add eu.po [Mikel Olasagasti] ○ po: update ca.po [Josep Puigdemont] ○ po: update sv.po [Daniel Nylander] ○ po: update fr.po [Michel Robitaille] ○ po: update tr.po [Nilgün Belma Bugüner] ○ po: update ja.po [Daisuke Yamashita] ○ po: update nl.po [Benno Schulenberg] ○ po: add pl.po [Andrzej Krzysztofowicz] ○ po: update da.po [Claus Hindsgaul] ○ po: update vi.po [Clytie Siddall] ○ po: update et.po [Meelis Roos] ○ po: update de.po [Michael Piefel] ○ po: update fi.po [Lauri Nurmi]	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• build-sys: release++ (-rc2) • mount: hint about helper program if device doesn’t exist. • rules: correct LSB init data for hwclockfirst.sh. • hwclock: check for ENODEV • mount: fix fd leak • sys-utils: Drop duplicate install of setarch manpage links. • agetty: drop useless and unused diff from upstream • hwclock.sh: drop redundant file pointer. • sys-utils: correct setarch.8 manpage link creation. • build-sys: remove hardcoded _GNU_SOURCE • mount: don’t call canonicalize(SPEC) for cifs, smbfs and nfs. • blockdev: add --getsz to blockdev.8 • meta: drop Conflicts: bsdmainutils too • cal comes from bsdmainutils as well. Drops Replaces: completely. • docs: fix ChangeLog URL • po: update hu.po (from translationproject.org) • losetup: fix errno usage • po: update po files • po: update fi.po (from translationproject.org) • mkswap: possible to crash with SELinux relabeling support • docs: add info about .bugfix releases and branches	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• build: don’t deliver col* and ul as part of bsdutils for now. • deliver hwclockfirst.sh on ubuntu as well. LP: #63175 • build: don’t deliver (emtpy) /usr/share/util-linux. • mount.8: Make package references be the actual binary package name in the distro. LP: #154399 • po: update de.po (from translationproject.org) • chsh: should use pam_end function to terminate the PAM transaction • po: update nl.po (from translationproject.org) • pg: fix segfault on search • mount: -L|-U segfault when label or uuid doesn’t exist • tests: fix blkid cache usage • script: dies on SIGWINCH. • chfn: add pam_end() call and cleanup PAM code • ionice: add a note about permissions to ionice.1 • script: dies on SIGWINCH • po: fix typo in de.po • po: update po files • setarch: generate groff links in a better way • Upstream git: ○ po: update sv.po (from translationproject.org) ○ mount: doesn’t drop privileges properly when calling helpers CVE-2007-5191 ○ hwclock: fix --rtc option.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ setarch: fix compiler warning ○ login: login segfaults on EOF (rh#298461) ○ build-sys: nls/locale handling in util-linux-ng general ○ blockdev: add missing description about option --report in manpage • fix messages in "hwclock.sh start". • Honor DEB_BUILD_OPTIONS=nostrip. • cfdisk.8: mention slang next to curses. • util-linux.postrm: remove /etc/adjtime on purge. • hwclock: Reintroduce hwclockfirst.sh on Debian machines. • mount.preinst: chroot-check was broken. • sparc-utils 'sparc64' binary sets ADDR_LIMIT_32BIT. • build: cfdisk doesn’t exist on some architectures. • build: look for fdisk in the right place. • flock.1: typo in man page. • mount: chain of symlinks to fstab causes use of pointer after free • Replaces: sparc-utils (for sparc{32,64}. • Don’t make rename.ul an alternative for rename. • Don’t deliver hexdump (bsdmainutils is newer). • Update bsdutils description. • Changes from upstream: ○ docs: update AUTHORS file	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ Revert "mount: improve error message when helper program not present" for translation freeze (reopens LP #131367) Will be fixed in 2.13.1 and 2.14. ○ taskset: check for existence of sched_getaffinity ○ setarch: add parisc/parisc64 support ○ mount: free loop device on failure ○ mount: avoid duplicates for root fs in mtab ○ build-sys: release++ ○ docs: update ReleaseNotes, update and sort AUTHORS file ○ po: update po/ stuff ○ ionice: clean up error handling ○ cytune: make the oneliner more specific the cyclades hw in question ○ docs: update TODO ○ setarch: add --3gb option for compatibility with Debian linux{32,64} command • Revert "umount: only call update_mtab if mtab_is_writable().", since the fix is already present in a different way. • Have debian/rules deal with architectures that don’t get packages. • debian/rules: cleanup and support nostrip option • build: fdisk (and therefore the udebs) do not get built on m68k. • build: /usr/bin/rename needs to be an alternative. • taskset: Don’t deliver taskset on m68k. • umount: only call update_mtab if mtab_is_writable(). • build: switch back to libblkid-dev for Debian.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Document git repository location • cytune.8: make the oneliner more specific the cyclades hw in question • control: Extend package descriptions. • Switch to debhelper, clean up delivery of binaries. • bsdutils: deliver more stuff that we build. Now partly Replaces: bsdmainutils and completely Replaces: linux32. • more upstream changes ○ docs: add DEPRECATED to EXTRA_DIST ○ docs: update AUTHORS file ○ docs: add note about http://translationproject.org ○ man-pages: cleanup of chrt.1 and taskset.1 ○ mount: improve error message when helper program not present ○ setarch: cleanup licensing note ○ setarch: add sparc32bash alias to keep compatibility with sparc32 ○ setarch: add *alpha* support ○ po: update de.po, vi.po, nl.po (from translationproject.org) • drop arch.1 man page. • deliver the right file for scriptreplay. • sfdisk: Allow drives over 2^31 sectors in size. • Deliver flock and flock.1. • hwclock.sh: Correct message.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			● cfdisk: switch back to slang2 ● setarch: add parisc/parisc64 support ● deliver setarch ● Fix distro check in debian/rules ● Use Breaks: on distros that support that in the previous release. ● Changes from upstream: ○ po: gettextizing some overlooked messages. ○ build-sys: add --disable-makeinstall-chown ○ docs: add README.licensing ○ tests: fix ULONG_MAX usage on 32bit machines ○ chsh: don't use empty shell field in /etc/passwd ○ more: fix underlining for multibyte chars ○ login: replace /usr/spool/mail with /var/spool/main in man page ● mount: make the error message a little more clear when a helper program is missing. (LP #131367) ● manpages: cleanup of chrt.1 and taskset.1. ● hwclock.sh: only report hwclock updated if we did that. ● update copyright to reflect README.licensing ● Merge ubuntu changes, do the right thing at build time. ● Go back to Depends: for the various packages, since the switch to libc5 is long, long over. ● Merge lpia support from ubuntu. ● Add lpia support back in. sorry.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• New debian version. Remaining ubuntu changes: ○ Add udev rule for calling /sbin/hwclock --hctosys dynamically: + debian/hwclock.rules, debian/hwclock.udev: Rule and script. + debian/rules: Install those. • mount should Suggest nfs-common, not Recommend it. • Fix build-depends for hurd-i386. • Merge ubuntu changes into a new Debian version. Remaining: ○ Add udev rule for calling /sbin/hwclock --hctosys dynamically: + debian/hwclock.rules, debian/hwclock.udev: Rule and script. + debian/rules: Install those. • New upstream version • If nfs-common is not installed, skip nfs check • More fixes from upstream: ○ swapon: cleanup fsprobe_*() usage ○ swapoff: correctly handle UUID= and LABEL= identifiers ○ mount: fix incorrect behavior when more than one fs type is ○ tests: add script(1) race condition test ○ script: fix race conditions ○ mkfs: remove nonsense from man page ○ blockdev: use LU and LLU for BLKGETSIZE and BLKGETSIZE64 ○ blockdev: fix "blockdev --getsz" for large devices • Merge ubuntu fixes into new Debian version. • More fixes from upstream	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• mount.preinst: deal with no /proc/mounts. • swapoff: handle UUID= and LABEL=. • mount.preinst: ○ check the right directory for mount.nfs. ○ look for ' nfs ' mounts. • switch to using libvolume-id-dev • Recommend: nfs-common so that portmap doesn’t become defacto-Required. NFS mounts will not work unless nfs-common is upgraded to at least the Recommended version, so now mount.preinst will fail if there are NFS mounts and no /usr/sbin/mount.nfs. • Merge ubuntu changes: ○ Add udev rule for calling /sbin/hwclock --hctosys dynamically: + debian/hwclock.rules, debian/hwclock.udev: Rule and script. + debian/rules: Install those. ○ use libvolume-id instead of blkid. This will be true for debian once a current enough udev is available. • add option for 8-bit chars in agetty. • Merge upstream fixes (rc2+git) • arch is dealt with upstream now. • Mention hfsplus in mount.8. • Add m32r. • use snprintf in logger.c. • Various typos in cfdisk.8. • cleanup copyright. • manpage typos.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• New upstream version • drop libselinux-dev build-dep on kfreebsd-amd64 • A little more kfreebsd cleanup • Fix nfs-common dependency • fix ionice build errors on several architectures. • no libselinux on kfreebsd-i386 • New upstream (util-linux-ng). ○ several patches were not ported forward from 2.12-19 ○ no kerneli support in crypto loop, since it is not in 2.6 kernels. ○ 20guesshelper: filesystem detection has been dropped. Mount is built with filesystem probing ○ 20xgethostname: does anyone care? ○ 30nfs*: NFS support has moved to nfs-utils, and removed from util-linux. Add Depends: nfs-common until Lenny ships. ○ umounting usb sticks as a user no longer segfaults. • Add LSB formatted dependency info in hwclock.sh. • Reflect Debian locations in getopt manpage. • Conflict/Replaces/Provides: schedutils. • README.Debian.hwclock needs a .gz in hwclock.sh. • Deliver tailf. • Deliver partx. • USB unmounting dereferenced a null pointer.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ Files: 70fstab.dpatch • Fix sparc disk label generation. This is required for LDOM and parallel installations with Solaris 10. Add patch: 80sparc-new-label Many thanks to David S. Miller for the patch. NOTE: users upgrading from older versions should re-run fdisk to update the disk label. • Merge from debian unstable, remaining changes: ○ Use volumeid instead of blkid to be able to access (mount/umount/swapon) volumes by UUID and/or label: + debian/control: libblkid-dev → libvolume-id-dev build dependency + debian/patches/70libvolume_id-support.dpatch: SuSE patch for using libvolume-id. ○ Add udev rule for calling /sbin/hwclock --hctosys dynamically: + debian/hwclock.rules, debian/hwclock.udev: Rule and script. + debian/rules: Install those. • mips/mipsel buildds use sudo. Fix install target so that mount.deb builds. • Stop printing erroneous "rpc.idmapd appears to not be running" message. Files: 30nfs4.dpatch. • debian/control: Update maintainer fields according to debian-maintainer-field spec. • Merge from Debian unstable. Remaining changes: ○ libvolume_id support patch from SuSE ○ single ubuntuized hwclock script • Userspace software suspend fix. • armel support. • actually apply 30swsusp-resume. And support userspace sw susp too. • Fix off-by-one issue in agetty -I. • Drop extraneous "again" from hwclock.sh and remove references to hwclockfirst.sh.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Drop PAGE_SIZE usage completely, use sysconf(_SC_PAGESIZE). • Make intr the default for NFS v2 & v3 mounts in addition to being the default for NFS v4. Thanks to Tollef Fog Heen for the idea. • New amd64 rdev patch. • Make that 11 for hwclock.sh, since we need / to be writable for the adjfile. • NFS seems to not like 127.0.0.1 as a client ID for everyone. ○ 30nfs4-setclientid.dpatch by Steinar H. Gunderson <sesse@debian.org> • Move hwclock.sh to 8 since localtime is now a file, not a symlink. Adds Depends: tzdata (>=2006c-2) • ship rdev on amd64. • drop hwclockfirst.sh, and put hwclock.sh back at 50. See #50572 and • Deal with _syscall5 going away. Patch imported from Ubuntu. • typos in NFSv4 (GSSDLCK didn't have .pid, and the latest nfs-common no longer creates the file at all.) ○ modified 30nfs4-fix.dpatch • NFSv4 patch fixes for cfs. Thanks to Trond Myklebust for the quick fix. ○ modified 30nfs4-fix.dpatch • Release NFSv4 support. • Deliver isosize. • Fix udeb dependencies. • Turn on fixed nfsv4 patch. Thanks to Steinar H. Gunderson <sgunderson@bigfoot.com> • Drop NFS v4 patch, since it breaks mounting things exported by nfs-user-server. It will be happily reapplied once someone fixes the patch.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ fix compiler warnings in said patch. ○ Apply nfs4mount.c fix to (dropped) nfsv4 patch. • Add nfsv4 patch. • make hwclock even more policy compilant. • make hwclock prettier. • Stupid fat-fingers typo. • Add ppc64 support. • Update sections to match the overrides file. • hwclockfirst.sh may not exit, since it gets sourced. • make the start messages from hwclock{first,}.sh slightly different, for clarity. • Build sparc binaries on sparc64 • Actually cleanup pager alternatives. • Deal better with long passwords. Based on patch from YAEGASHI Takeshi <yaegashi@debian.org>. • Add back in dropped cramfs-udebsize patch. • New upstream verison and maintainer. ○ cfdisk: fix a segfault with ReiserFS partitions ○ umount: disallow -r option for non-root users (CAN-2005-2876) ○ sfdisk: document -G option in --help output ○ updated translations: ca, et, fr ○ sfdisk: add -G option (Andries Brouwer) ○ updated translations: de, es, ru, sv, tr, nl	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• split cfdisk into its own udeb. • Really move hwclockfirst.sh back to S18 where it belongs. Put hwclock.sh at S22. See #50572. • Missing line break in hwclock.sh. • Include swap-suspend patch from Ubuntu. • Fix variable name typo in hwclock.sh. • Add CPU=$(arch) to make call for building on amd64/i386 mixed systems. • Cleanup lsb_init function usage. • if /etc/adjtime is a dangling symlink, don't use it in hwclock*.sh • Applited patch by Max Vozeler to fix a local privilege escalation vulnerability in umount -r [debian/patches/51security_CAN-2005-2876.dpatch] • Fix non-posix typo in hwclock.sh. • Use helper program in mount for guessed FS types too. Thanks to Manish Singh and Fabio Massimo Di Nitto. Adds: 20guesshelper.dpatch • Remove /usr/doc links on install. • Fix /usr/bin/pg pager alternative. • Overhaul hwclock.sh and hwclockfirst.sh. • Resync with Ubuntu, changes by Martin.Pitt@ubuntu.com: debian/patches/60_opt_O1.dpatch: ○ MCONFIG, configure: Build with -O1 instead of -O2 to work around cfdisk segfault. ○ Yay for upstream build systems which do not support specifying CFLAGS or OPT without breaking. • Merge changes from ubuntu ○ closes #319143	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Build-Depend: libslang2-dev. • dpkg-architecture says DEB_HOST_GNU_SYSTEM is "linux-gnu" now, not "linux". Take account of this, and add compatibility code for old dpkg-architecture • Don’t special case sparc, it has umount2. • Run hwclockfirst.sh after modules load, so that rtc is loaded. • Resynchronise with Debian. • correct shutdown message from hwclock.sh • Depend on newer libblkid1. • Add an alternative for pager pointing at pg (at pref 10). • enable fdisk on s390. • Update dependencies for new libblkid1 • Resync with Debian. • Really fix man page in alternatives. • more typos in hwclockfirst.sh. • Resync with Debian. Closes warty #3366, 4784 • New upstream version. (2.12p) ○ cfdisk: fix number of new partition when partitions not in disk order ○ fdisk: fix Sun label handling in sector mode ○ mkfs: never truncate filename (not that that ever happened) ○ more: fix redraw flaw. • New upstream version. (2.12o)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ lomount: revert patch from 2.12j ○ lptune.8: -T option is obsolete ○ mkswap, mkswap.8, swapon: support labels (use HAVE_BLKID=no as long as the blkid library doesnt support this) ○ umount: allow user unmounting repeatedly mounted nfs mounts ● Build-Depend on uuid-dev. ● correct chown args in debian/rules. ● include man page in update-alternatives for pager. ● fix typos in howclockfirst.sh. ● fix losetup -N documentation. ● cleanup some narrow window sprintf issues in cfdisk. ● Resync with Debian. ● New upstream version ○ cfdisk: recognize JFS, support reiserfs labels (flavio.stanchina@tin.it) ○ mount: fix option parsing bug ○ mount.8: several updates ○ swapon.8: document -v option ● Resync with debian ● New upstream version, shrinking the size of the Debian diff. ○ Makefile: remove cat-id-tbl.c upon make clean ○ fdisk: fixed a bug that would cause a non-update of a sun disklabel	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ fdisk: use sectorsize instead of 512 for SGI (Eric Y. Theriault) ○ fdisk: use *attribute*packed for alpha, ARM: avoid unaligned accesses ○ hwclock: actually use HAVE_tm_gmtoff ○ swapon: fix priority handling ○ umount: refuse to unmount an empty string • Jetisoning the (broken) hurd patch for now. • Resync with Debian • Switch to dpatch. • Clean up --nohashpass in losetup. • Use stat instead of open in losetup. (From #285353) • Resync with Debian • New upstream version. • various translation updates • gcc-3.4 support help • Resync with Debian • umount -l "" does bad things. Don’t do let the user do that. • remove non-utf8 characters from changelog. sorry. • resync with Debian • uninitialized variable. • resync with Debian • New upstream version	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• resync with debian. • mkswap on a file was broken. Thanks to Bas Zoetekouw <bas@debian.org> for the patch. • add libblkid-dev to Build-Depends. • Resync with debian. Fix mount segv. • Fix mount segv’s. • Fix unterminated string in hwclock.sh (thanks, Jones Lee). • Re-sync with Debian. • Cleanup the changelog entry in the uploaded package, to reduce panic. • Even newer upstream… sigh. • Fix copyright file. • New upstream. • Add amd64 to fdisk. • use absolute path to hwclock in scripts. • deal with unaligned partition table entries in fdisk. • The "SO WHY IS LETTING TWO PROCESSES OPEN THE SAME TTY FOR READ A *GOOD* THING" Release. • Admit that the kernel API doesn’t provide what we need, and turn the code back off. Discussions will follow on how to deal with this post-sarge. • The I-HATE-LINUX-TTY-HANDLING Release • New and improved tty-in-use check, that actually works. • Fix tty-in-use check. Many thanks to Samuel Thibault for tracking this down and providing a patch.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Have pri= only affect that entry in swapon -a. • Mention the freshmeat site. • fix disk sun label creation in fdisk. • Use a more general form for uname. • Provide fdisk-udeb for sparc. • Cleanup vty code in getty. • Changes from Javier Fernandez-Sanguino Pen~a <jfs@computer.org> ○ Added amd64 architecture ○ Fixed manpage to avoid pointing to non existant files ○ Fixed Theodore Tso's address to the new one in dmesg ○ Modified cfdisk's es.po in order to not ask for an accented character since it will not be shown in cfdisk and causes confusion amongst users, this change could be reverted when upstream manages 8-bit characters better ○ mkswap manpage now mentiones --sparece=never option to cp ○ Added upstream maintainers to debian/copyright • Clean up FTBFS isses. • Deal with hwclock.sh on s390x. • Have getty check before opening a device. • Fix compile error in get_blocks.c. • Help out fdisk-udeb. • Version the build-depends on slang1-utf8-dev to make life clearer for woody backporters… • Deliver pg.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Re-add support for kerneli (if cryptoapi is there, we use it. If not, we assume that -e <name> refers to kerneli). • release to unstable. • Fix package priorities. • Cleanup cryptoapi patch. (Really just needed the keybits patch.) • New upstream release. • cryptoapi patch (sort of) migrated forward, along with code inspired by the patch in #206396. Still fighting with 2.4.22 crypto api, patches welcome. • Fix mount -p (to make -p an accepted option), and add back in okeybits= to make the natives happy. • Merge in dependency change from -4.1, and cleanup the dirty diff that brought. • Was creating invalid swap files. • Fix LSB failures in cal. • Fix wall copyright, patch from Shaul Karl. • Fix HURD patch. • Include cramfs support. • Fix configure bug. • Create /etc/mtab mode 0600. • Fix man page ref to rpc.nfsd(8). • Non-maintainer upload. • Correct build-depend from slang1-dev to slang1-utf8-dev to get cfdisk in fdisk-udeb to link with the same slang library as the other d-i modules. Patch from Joe Nahmias. • Put ddate back in, just to keep the natives quiet.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Fix bashism in postinst from hurd port. • Drop ddate. • Clean up messages in hwclock.sh. • Some package description changes. • properly install changelog. • Fix hwclock man page reference to /usr/local/timezone. • add in hurd patch. • Actually fixed in 2.11z-1 (or earlier)… • Install line. • Suggest dosfstools (home of mkfs.vfat). • New upstream version. • Fix sparc build. sigh. • New upstream version • don’t build fdisk on m68k. • Honor HWCLOCKACCESS in hwcolockfirst.sh. • New upstream version. • Include errno.h where needed. • Fix changelog. • New upstream release • Incorporate udeb fix from Tollef Fog Heen. • Build fdisk-udeb only where we built fdisk…	

Date	Package	CVE(s)	Synopsys	Hardware Version
			● NMU with maintainer's permission ● Generate udeb with *fdisk in it. ● New maintainer. ● Fix Standards-Version. ● Loosen dependency of util-linux-locales to match upstream version. ● Orphaned this package. ● Applied a patch to hwclock/cmos.c that should fix the compilation on alpha. ● New upstream release. ○ It's now possible to build pivot_root on all architectures. ○ The confusing error message in mount is fixed. ○ minix v2 filesystems are now autodetected by mount. ○ tmpfs is now documented in mount (8). ○ s/top/Top/g in ipc.texi. ● New upstream release. The following bugs are fixed in this release: ○ "setterm -foreground default" does work now. ○ "more" on empty files does no longer print junk on powerpc. ○ The entry in the expert menu the option to create a SGI disklabel is now called "create an IRIX (SGI) partition table". ● debian/rules: "raw" does now compile on m68k. ● Remove the special handling for PowerPC/PReP machines from the postinst.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Corrected the bug introduced in the last upload that did let the installation of util-linux fail on powerpc. • s/"uname -m"/uname -m/ in the postinst of util-linux. • Don’t install debian/tmp/DEBIAN/conffiles on s390 (since there’s no longer a hwclock on s390). • Don’t install hwclock on s390. • Make the warning in hwclockfirst.sh that occurs when the timezone couldn’t be determined more silent. • New upstream release that consists of bug fixes and several security fixes. ○ renice does no longer incorrectly report a priority of 20. ○ Upstream has included the "replay" script written by Joey Hess <joeyh@debian.org>. • Added a hwclockfirst.sh script that runs before S20modutils. • New upstream release. ○ This release contains some fixes in more (1). • Don’t build pivot_root on ia64 (ia64 has broken kernel headers). • m68k doesn’t has pivot_root, too. • Don’t build "raw" on m68k because it doesn’t compile. • hwclock.sh does now check $HWCLOCKACCESS. • New upstream release. • fdisk does now know about the partition type of the Linux/PA-RISC boot loader. • New upstream release. Bugs fixed in this release: ○ Fix for big endian architectures in disk-utils/raw.c.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ Support for SuperH in mount. ○ The alpha options in hwclock do now work as documented. ○ mount (8) does now mention that the quota utilities do use the *quota options in /etc/fstab. • New upstream release. This release contains fixes for the following bugs: ○ Different fix for the problems with the "user" option in umount. ○ Support x86 RTC on UltraSPARC III’s. ○ An error message in mount is now proper english. • Install more.help in /usr/share/util-linux. • Updated README.Debian.hwclock.gz. • Corrected the "charset" in po/nl.po . • Standards-Version: 526.7.8.9.13-Foo.6 • Made util-linux-locales binary-all. • Applied a fdisk patch for hppa and added hppa to fdisk_arch in debian/rules. • Fixed the bug in umount that did let a user umount a file system mounted by root when the "user" option is set in /etc/fstab. • Corrected a build error on powerpc in debian/rules. • Corrected in util-linux-locales: Section : base → utils Priority: required → optional • Added the crypto patch again. Fixed in the new crypto patch: ○ It’s now the complete crypto patch. ○ "losetup" no longer lists the available ciphers.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ It already includes the patch from #68804. • Added blockdev to util-linux. • Include pivot_root in util-linux. • Added a lintian override for mount and umount. • New upstream release. This release fixes the following bugs: ○ the problem with extended partitions when using the "o" command in fdisk is fixed ○ adfs options are now documentated in mount (8) ○ missing .TP in mount (8) was added • The locales are now in a seperate util-linux-locales package that is not essential. • util-linux "Suggests: kbd | console-tools" to help people to find where "kbdrate" is. • Added support for devfs in rdev. • Include the "raw" program in util-linux. • Include fdformat again. • Moved the "install-info" call from the postrm to the prerm. • Install "HOSTORY" as "changelog.gz" in all packages. • Removed the "swapdev" link to "rdev". Upstream says about swapdev: Nevertheless, all this is ancient junk. I just checked swapdev and found that it was last used in kernel 0.12 but that swapdev (or rdev -s) has not done anything in any kernel later than 0.12. • Corrected the location of the examples in getopt (1). • Added the missing build dependency on gettext. • Added mips, mipsel and ia64 to fdisk_arch in debian/rules.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- New upstream release. - This release contains a fix for an overrun sprintf in mount. - A message of cfdisk is less confusing in this release. - Don’t include a group writable /usr/share/locale/da . - New upstream release. - Upstream removed "kbdrate" from util-linux (it’s now in the packages kbd and console-tools). Let util-linux conflict with kbd (<< 1.05-3) and console-tools (<< 1:0.2.3-21) to avoid that a user of these packages has a system without "kbdrate". - New maintainer. - New upstream release, - login-utils/wall now checks whether the devices has a colon in it and skips it if it does. This prevents wall from trying to send to X connectiosn. - added joeyh’s script patch for handling SIGWINCH, - debian has long been modifying the man page to point at proper file locations, these two bugs were merged with two other bugs that are actually bugs in docs v. reality and so were not getting closed. unmerged and are now being closed. - DEB_HOST_ARCH is set if not run from within dpkg-buildpackage, - devfs code now in the upstream, - upstream fixed the wrong NAME, - umount knows that mips does not support umount2, - removed calls to suidregister - orphaning package - New upstream release	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• New maintainer (possibly temporarily) • I left out the alpha fdisk patch and the crypto patch. Debian needs to line up with the upstream. If there is demand, will see what I can do. • has patch for autofs from #31251, • loop mounts leaking seems to have been fixed long ago, • nfs(5) updated to mention (no)lock option, • umount sigsegv’ing when user lacks permisions seems to have been fixed long ago, • FHS transition started in last upload forgot to, • umount -f is now documented and tries to be functional, • for all of those "please update this package" bugs, • umount -f seems to work now, I believe it was a kernel issue, • bsdutils description cleaned, no longer refers to missing binaries, • Patch rejected by upstream, • problems with alpha and bsd partitions believed fixed in 2.9w, • /dev/vcsa patch accepted, • msglevel fixed by upstream, • update-mime call seems to have been fixed in previous release, • looks like user error, • does not look valid any more, • LVM supported in current release, • forgot to • prerm typo, oops,	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• fdformat is just a wrapper, no more confusing messages, • hwclock.sh supports a BADYEAR argument from etc/default/rcS. • no longer include example.files, they do not readily apply to debian • New upstream release • NMU with maintainer’s permission • added Build-Depends, • upstream added the patch from #36340, so • upstream put '--More--' back to reverse video, • hwclock man page points at /usr/share/zoneinfo, not usr/lib • all created packages' postints now sets usr/doc/ symlink, its prerm removes said link • copyright file now points to usr/share/common-licenses and the typo in the URL was fixed (it is misc, not Misc) • update hwclock.sh to reflect FHS changes • debian/rules file brought up to date for FHS • elvtune man page put with the binary • The above changes allow • edited fr.po, fixed "Nombre de partitions" to "Numero de partition", • whereis knows that /usr/share/man/* is valid, • debian/rules now sets SHELL to bash, so it can use bashisms, • upstream HISTORY file included as changelog.gz, • removed /etc/fdprm,	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• made fdformat a sh script instead of a bash script (the bash was unneeded) • New upstream code. Add elvtune. • New upstream code. • Non-Maintainer Upload • Patch from Ben Collins to fix the -v[01] option in mkswap • Patch from Chris Butler to fix hwclock's handling of RTC • Change to line 879 of fdiskbsdlabel.c to allow building on sparc (patch sent to maintainer) • Patch from David Huggins-Daines <dhd@linuxcare.com> which is required to get a working fdisk on alpha. • Patch for mips support from Florian Lohoff <flo@rfc822.org>. • included patch from David Huggins-Daines <dhuggins@linuxcare.com> so that fdisk behaves correctly with OSF/1 disklabels. • `(Important bug)` `* Now that 2.10f-1 has been tested in unstable, re-upload it to frozen.` • New upstream release: • Security fix for mount (okir) • Avoid infinite loop in namei (Brett Wuth) • added clock-ppc.c (from Matsuura Takanori), not merged yet • deleted clockB subdirectory • recognize mkdosfs string (Michal Svec) • New: rename • Added option to mkswap so that user can override pagesize	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• fdisk -l now reads /proc/partitions when no device was given • Fixed fdisk.8 (James Manning) • Added devpts info to mount.8 (Elrond) • Newline fix for logger output to stdout (Henri Spencer) • There is no real concensus about what we should do about the hwclock issue. Now at least the problem is enough documented to let the user decide. (Thanks to Henrique M Holschuh <hmh+debianml@rcm.org.br> for the patch). When this package is installed, I’ll examine one by one which BR can be closed. • kbdrate isn’t suid anymore. • Included patch from "J.H.M. Dassen (Ray)" <jhm@cistron.nl>: ○ Restored enhanced losetup(8) manpage. ○ Restored encrypted filesystem support, by applying util-linux-2.9w from patch-int-2.2.13.3.gz as found on ftp.kerneli.org (modified to work with Debian’s kernel-patch-int’s crypto.h). • Recompiled with ncurses5. • ipcrm now accepts multiple ids thanks to a patch from Topi Miettinen. • fix postinst script: • Disabled 'hwclock --adjust' on boot. • cfdisk must be build with slang; not ncurses. • New upstream release. • Put renice manpage in section 1 instead of 8. • kbdrate’s PAM now uses pam_unix.so by default. • already fixed in 2.10-5: • Patch by Topi Miettinen <Topi.Miettinen@nic.fi> to a longstanding bug in logger.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• replace fdformat by a notice asking to use superformat instead. • remove setfdprm; • conflict/replace with fdisk on sparc. • re-introduce missing c?fdisk… (oops ;) • Do TheRightThing(tm) for bug #47219. • from NMU prepared by Torsten Landschoff <torsten@debian.org>: • Fixed case expression in hwclock.sh • Added usage information to hwclock • Upstream has long changed mount.c to handle nouser properly • Excluded clock.8 link from powerpc build • Replaced "$(shell dpkg --print-architecture)" with "$DEB_HOST_ARCH" in debian/rules. • New upstream release. • make /etc/rc{0,6}.d/*hwclock.sh correctly. • Correct kdbrate pam entry. • Fix fdiskdsblabel.h. • Use jgg’s patch for hwclock.sh • Really link kbdrate with pam. • New upstream release. • Include PowerPC patch from Matt Porter <mporter@phx.mcd.mot.com>. • Should be 100% PAMified(tm). Please report anomalies.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• updated losetup.8 from "J.H.M. Dassen (Ray)" <jdassen@wi.LeidenUniv.nl>. • Upstream upgrade: util-linux 2.9w: • Updated mount.8 (Yann Droneaud) • Improved makefiles • Fixed flaw in fdisk util-linux 2.9v: • cfdisk no longer believes the kernel's HDGETGEO (and may be able to partition a 2 TB disk) util-linux 2.9u: • Czech more.help and messages (Jii Pavlovsky) • Japanese messages (Daisuke Yamashita) • fdisk fix (Klaus G. Wagner) • mount fix (Hirokazu Takahashi) • agetty: enable hardware flow control (Thorsten Kranzkowski) • minor cfdisk improvements • fdisk no longer accepts a default device • Makefile fix • now uses the script(1) supplied with util-linux instead of the one from the old bsdutils package. • remove alpha specific build patch: • remove useless warning in preinst. • include missing fdformat, setfdprm. (How comes nobody noticed yet?!) • recompile against slang1-dev 1.2.2-3. • correct hwclock.sh;	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Non-maintainer upload. • Applied util-linux-2.9s.patch from patch-int-2.2.10.4.gz as found on ftp.kerneli.org to enable support for mounting encrypted filesystems through the loopback devices when using an international kernel. (Fixes: Bug#36939, #38371) • Include <linux/loop.h> and <linux/crypto.h> in the source, so as not to rely on source outside main. • Updated the losetup(8) manpage. • Upstream upgrade: • national language support for hwclock • Japanese messages (both by Daisuke Yamashita) • German messages and some misc i18n fixes (Elrond) • Czech messages (Jii Pavlovsky) • wall fixed for /dev/pts/xx ttys • make last and wall use getutent() (Sascha Schumann) [Maybe this is bad: last reading all of wtmp may be too slow. Revert in case people complain.] • documented UUID= and LABEL= in fstab.5 • added some partition types • swapon: warn only if verbose • changed hwclock.sh to get rid of a lintian error. • Added missing *.gmo files • Re-add Harmut’s powerpc patch that somehow got left out • Fix stupid bug #37916. • Upstream upgrade.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Now compiled with PAM=yes. • initial .it localisation. • Improved .fr translation. • corrected hwclock.sh (reassigned #35429 back to sysvinit). • put rev into /usr/bin instead of /usr/sbin (Fix #34188,#35421). • include getopt examples (Fix #34705). • Upstream upgrade. • This source package now also provides the 'bsdutils' binary package. • Included patch for logger.1 from and1000@debian.org. • Included patch to logger.c from Joey • renice.c: include <errno.h> • re-use script(1) from the 'old' bsdutils package as well as README.script • Now umount is compiled with '-f' support • Re-add suidregister support for mount • modify mount.8 manpage to warn that nosuid is useless if something like suidperl is installed. (doesn’t fix the critical bug #31980 reported on suidperl, but at least warn about its existance) • add missing manpages (ramsize,rootflags,swapdev) • #32414: changed a 'rm' into 'rm -f' so the source package builds cleanly. • also target the upload for frozen since this is the only missing package to be able to safely use kernels 2.2.x: To the FTP/Release maintainers: util-linux_2.9g has been introduced in unstable on Dec, 31st 98; so far I received no bug reports about it except for the missing manpages. Also compared to the 2.7.1 version from frozen, this package fixes *57* bugs. (see www.debian.org/Bugs/db/pa/lutil-linux.html)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Fix bug #31981. • Localised cfdisk + provided initial French translation. New translations welcome; you can get the potfile at http://www.ldsol.com/~vincent/util-linux.pot • Add rev and readprofile commands. • Updated fstab.5 regarding spaces in mount points names. • Fix bugs #32235,#31997 (missing hwclock.8 manpage). • Fix bug #32097 (missing mkswap.8 manpage). • Improve somewhat cfdisk regarding exit codes thanks to Enrique’s patch (#31607). • Include patch from Hartmut Koptein for better powerpc support. • Patch from Topi Miettinen (Thanks Topi ;) to fix bug #31554,#31573. • Adopting the package from Guy Maor. • Re-add hwclock & kbdrate which had been lost (Fix bug #31476). • YA NMU. • Split mount out into separate package so as not to force the dangerous replacement of an essential package. • NMU (Part II): Fix more problems in 'mount'. • swapon now warn if swap device has insecure mode; Patch from Topi Miettinen <tom@medialab.sonera.net> (Fix bug #23249). • mount can now handle multiple hostnames for NFS mounts in fstab (Fix bug #29309). • Do’h; add missing /sbin/swapoff ;). • NMU. • This package now provides /bin/mount & co. and thus obsoletes the mount package.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• provides the ddate command (Fix bugs #30015 & #19820). • Move wtmp lockfile from /etc to /var/lock (Fix bug #29128). • Set bug #28885 to 'fixed' (this-is-not-a-bug,-but-a-feature(tm)). • Set bug #27931 to 'fixed' (works again since version 2.8). • Set bug #27723 to 'fixed' (been fixed by the ARM NMU). • Set bug #25831 to 'fixed' (hwclock now works as advertised). • Set buffering off on the output channel in chkdupexe.pl (Fix bug #22839). • Include patch for powerpc build by Joel Klecker <jk@espy.org> (Fix bug #21374). • Removed the confusing references to agetty (Fix bug #20668). • Check the result for the malloc()s added in the code to chown vcsa to root.sys (Fix bug #18696). • Include patch for sparc build by Eric Delaunay <delaunay@lix.polytechnique.fr> (Fix bug #17784). • Set bug #17752 to 'fixed' (Appear to work with current versions of xvt and /bin/more). • Include patch for alpha build by Christopher C Chimelis <chris@classnet.med.miami.edu> (Fix bug #17661). • Patch mkfs.minix doesn’t go into infinate loop any more depending on the argument passed to -i (Fix bug #17648). • Set bug #17483 to 'fixed' (now that util-linux is compiled with libc6 > =2.0.6 it should be fixed). • Set bug #26625 to 'fixed' (this patch has already been applied). • Applied patch from Bcwhite to get mime support (Fix bug #26715). • Applied patch from Topi Miettinen <tom@medialab.sonera.net>: POSIX etc fixes:	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ ioctl(.., TCSETSF,..) → tcsetattr() ○ ioctl(.., TCGETS,..) → tcgetattr() ○ ioctl(.., TIOCGPGRP,..) → tcgetpgprp() ○ gcc -Wall warning fixes ○ write(2, ..) → write(fileno(stderr), ..) ○ vi → sensible-editor ○ added setlocale(LC_ALL, "") ○ use perror, isdigit, isprint, iscntrl where applicable ○ execv → execvp ○ added simple ELF detection OpenBSD fixes: ○ UCB fix ○ POSIX: rindex → strrchr ○ obsolete fseek flag L_SET → SEEK_SET ○ control-F == f ○ $EDITOR support (Fix bug #27635). • Link clock.8.gz to hwclock.8.gz (Fix bug #25852). • Non-maintainer upload. • Recompiled with slang1. • Non-maintainer upload • Include /etc/init.d/hwclock.sh • Fix some of the (pre|post)(inst|rm) script wrt $1 processing Fixes: #18007: sysvinit: hwclock.sh uses GMT env variable - but how? #26904: hwclock.sh doesn’t "test -x" #24649: [Peter Kundrat <kundrat@gic.sk>] hwclock startup script #20728: util-linux: hwlock:	

Date	Package	CVE(s)	Synopsys	Hardware Version
			GMT status lost? #19248: util-linux should install /etc/init.d/hwclock.sh • NMU: Added ARM architecture in 'disk-utils/fdiskbsdlabel.h' and 'disk-utils/fdiskbsdlabel.c'. • Removed '-m3' flag from arm-specific optimizations in MCONFIG. • Non-maintainer upload - new 2GB swap areas, removed hostid • upstream uses fixed more.c (line 813 had *p++) • Non-maintainer upload • recompiled with slang1 and ncurses4 • Another m68k patch from Roman Hodek <rnhodek@faui22c.informatik.uni-erlangen.de> • fdisk patch from Russell Coker <rjc@snoopy.virtual.net.au> for better behavior on IDE CD's when HDIO_GETGEO fails. • fix getopt(1) typo. (16227) • Use slang for cfdisk. • fdisk -l tries eda also (13841). • Fix fdisk -l segfaults (15236,15603). • Install rdev on only i386 (15228). • Don't strip perl script (15480). • Add type 17=Hidden IFS to cfdisk (16843). • Removed sync (13291). • Added m68k hwclock patches from Roman Hodek (9870). • agetty.c: set vcs,vcsa to root.sys 600 when starting. • libc6 compile of new upstream version (10098, 11744, 13123).	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Updated cfdisk to cfdisk 0.8k • Added old patches; I'll send them upstream. • fdisk - extended paritions, exit on EOF. • mkfs - fix search paths. • mkfs.minix - set owner of root dir to invoker. • chkdupexe - remove upstream brokenness by checking PATH too. • mcookie - fix man page • whereis - fix search paths, find .gz files. • sync - put it back (doh!) • Folded in getty: • glibc patch (8815, 11687, 12738). • Set tty to 660 root.dialout (8960). • Register pager alternative (12475). • Updated cfdisk to ftp.win.tue.nl:/pub/linux/util/cfdisk-0.8i.tar.gz • Updated cfdisk to ftp.win.tue.nl:/pub/linux/util/cfdisk-0.8g.tar.gz (#9146) • -i from 2.5-9 removed as no longer needed. • cfdisk: really fixed cast this time so should be able to deal with >2GB disks(#6747, #8041) • fdisk, cfdisk: Added partition id 0xa6 = OpenBSD (#7571) • setterm: use putp to output (#7852) • Removed miscutils removal trick as it no longer works (#5757, #6862)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• mkfs.minix: added patch from Volker Leiendecker <volker@fsing.uni-sb.de> to set owner of root directory to invoker (like mkfs.ext2). (#6902) • Fix dpkg-shlibddeps rules line for m68k (#5818) • Add undocumented "-i" flag to ignore bad partition tables when starting instead of throwing a fatal error. Let’s pass this to the upstream maintainer, please. • disk-utils/cfdisk.c: cast sector number to ext2_loff_t in calls to ext2_llseek() • sys-utils/clock.c: fixed bug on machines without RTC enabled. • sys-utils/whereis.c: better path, compare function. • Install whereis, cytune, setsid. • sys-utils/clock.c: Fixed bugs when real-time clock device is enabled in kernel. • New source format. • disk-utils/fdisk.c: Added type a7 = NEXTSTEP (fixes bug 3259) • fdisk.c,cfdisk.c: Applied patch from Miquel van Smoorenburg <miquels@Q.cistron.nl> to let fdisk and cfdisk support Linux extended partitions. • Applied patch from Frank Neumann <Frank.Neumann@Informatik.Uni-Oldenburg.DE> for Linux/m68k support. • Install mkcookie. • disk-utils/mkfs.minix: fixed bug 3777 re parsing oddities. • misc-utils/setterm.c (tc_entry): Applied patch from Michael Nonweiler <mrn20@hermes.cam.ac.uk> to make it work with ncurses. • misc-utils/chkdupexe.pl: Fixed some bugs with duplicate path and symbolic links. Put in a better value for exedirs. • Install chkdupexe, setterm.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- text-utils/more.c (getline): more now handles files with lines ending with "\r\n". Fixes Bug #2579. - Added 'priority: required' - disk-utils/fdisk.c (read_line): EOF now exits instead of looping forever. Fixes Bug #1206. - Added 'section: base' - Initial release	
2024-08-28	libtommath0	CVE-2023-36328	- Non-maintainer upload by the Debian ELTS team. - CVE-2023-36328: Prevent a series of integer overflow vulnerabilties that could have led attackers to execute arbitrary code and/or cause a denial of service (DoS). - Continuous integration changes: - Add a debian/.gitlab-ci.yml. - Add blhc failures in CI workflow.	M400 M410 R100E R100NA S1600E S100
2024-09-29	libexpat1	CVE-2024-45490 CVE-2024-45491 CVE-2024-45492 CVE-2023-52425 CVE-2022-43680 CVE-2022-40674 CVE-2022-25235 CVE-2022-25236 CVE-2022-	- Non-maintainer upload by the ELTS Team. - Fix CVE-2024-45490: xmlparse.c does not reject a negative length for XML_ParseBuffer(), which may cause memory corruption or code execution. - Fix CVE-2024-45491: Integer overflow for nDefaultAtts on 32-bit platforms. - Fix CVE-2024-45492: Integer overflow for m_groupSize on 32-bit platforms. - Backport NULL checks from upstream version 2.2.1. - Non-maintainer upload by the ELTS Team. - Enable test-suite in d/rules.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		25313 CVE-2022-25315 CVE-2022-25236 CVE-2022-23852 CVE-2021-46143 CVE-2022-22825 CVE-2022-23990	• Backporting patch for CVE-2023-52425 - DoS (resource consumption) parsing really big tokens due to $O(n^2)$ complexity. • Non-maintainer upload by the ELTS Team. • Add patch to fix heap use-after-free after overeager destruction of a shared DTD in function XML_ExternalEntityParserCreate in out-of-memory situations. (Fixes: CVE-2022-43680) • Non-maintainer upload by the ELTS Team. • CVE-2022-40674 heap use-after-free issue in doContent() (based on the backport for Bullseye made by Laszlo Boszormenyi) • debian/rules: add run of testsuite (but leave it deactivated as I only tested on amd64) • Non-maintainer upload by the ELTS team. • Run the upstream tests during the build. • CVE-2022-25235: arbitrary code execution due to malformed 2- and 3-byte UTF-8. • CVE-2022-25236: arbitrary code execution due to namespace-separator characters. • CVE-2022-25313: stack exhaustion in build_model. • CVE-2022-25315: integer overflow in storeRawNames. • Include follow-up fix for CVE-2022-25236. • Fix build issue in the tests of CVE-2022-23852. • Non-maintainer upload by the ELTS team. • Fix CVE-2021-46143, CVE-2022-22822, CVE-2022-22823, CVE-2022-22824, CVE-2022-22825, CVE-2022-22826, CVE-2022-22827, CVE-2022-23852, CVE-2022-23990 and CVE-2021-45960. Multiple security vulnerabilities have been discovered in Expat, the XML parsing C library. Integer overflows or invalid shifts may lead to a denial of service or other unspecified impact.	

Date	Package	CVE(s)	Synopsys	Hardware Version
2024-10-06	libgtk2.0-common	CVE-2024-6655	- Non-maintainer upload by the ELTS Team. - CVE-2024-6655: Stop looking for modules in the current directory	M400 M410 R100E R100NA S1600E S100
2024-10-06	libgtk2.0-0	CVE-2024-6655	- Non-maintainer upload by the ELTS Team. - CVE-2024-6655: Stop looking for modules in the current directory	M400 M410 R100E R100NA S1600E S100
2024-10-24	perl-modules	CVE-2020-16156 CVE-2023-31484	- Non-maintainer upload by ELTS team - Fix CVE-2020-16156: An attacker can prepend checksums for modified packages to the beginning of CHECKSUMS files, before the cleartext PGP headers. This makes the Module::Signature::_verify() checks in both cpan and cpanm pass. Without the sigtext and plaintext arguments to _verify(), the _compare() check is bypassed. This results in _verify() only checking that valid signed cleartext is present somewhere in the file. - Fix CVE-2023-31484: CPAN.pm does not verify TLS certificates when downloading distributions over HTTPS. - Fix follow up failure in testsuite.	M400 M410 R100E R100NA S1600E S100
2024-10-24	perl-base	CVE-2020-16156 CVE-2023-31484	- Non-maintainer upload by ELTS team - Fix CVE-2020-16156: An attacker can prepend checksums for modified packages to the beginning of CHECKSUMS files, before the cleartext PGP headers. This makes the Module::Signature::_verify() checks in both cpan and cpanm pass. Without the sigtext and plaintext arguments to _verify(), the _compare() check is bypassed. This results in _verify() only checking that valid signed cleartext is present somewhere in the file. - Fix CVE-2023-31484: CPAN.pm does not verify TLS certificates when downloading distributions over HTTPS. - Fix follow up failure in testsuite.	M400 M410 R100E R100NA S1600E S100
2024-11-21	libglib2.0-data	CVE-2024-52533 CVE-2024-34397	- Non-maintainer upload by the ELTS Team. - CVE-2024-52533: SOCKS4a proxy buffer overflow	M400 M410 R100E R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
		CVE-2023-29499 CVE-2023-32611 CVE-2023-32665 CVE-2021-3800 CVE-2021-28153 CVE-2021-27218 CVE-2021-27219	• Non-maintainer upload the ELTS team. • Fix CVE-2024-34397: Alicia Boya Garcia reported that the GDBus signal subscriptions in the GLib library are prone to a spoofing vulnerability. A local attacker can take advantage of this flaw to cause a GDBus-based client to behave incorrectly, with an application-dependent impact. • Non-maintainer upload by the ELTS Team • Add debian/salsa-ci.yml using lts-team/pipeline for jessie • CVE-2023-29499: GVariant deserialization fails to validate that the input conforms to the expected format, leading to denial of service. • CVE-2023-32611: GVariant deserialization is vulnerable to a slowdown issue where a crafted GVariant can cause excessive processing, leading to denial of service. • CVE-2023-32665: GVariant deserialization is vulnerable to an exponential blowup issue where a crafted GVariant can cause excessive processing, leading to denial of service. • CVE-2021-3800: information leak using CHARSETALIASDIR envvar. • Non-maintainer upload by the ELTS team. • Fix CVE-2021-28153: When g_file_replace() is used with G_FILE_CREATE_REPLACE_DESTINATION to replace a path that is a dangling symlink, it incorrectly also creates the target of the symlink as an empty file, which could conceivably have security relevance if the symlink is attacker-controlled. (If the path is a symlink to a file that already exists, then the contents of that file correctly remain unchanged.) • Fix CVE-2021-27218: If g_byte_array_new_take() was called with a buffer of 4GB or more on a 64-bit platform, the length would be truncated modulo 2**32, causing unintended length truncation. • Fix CVE-2021-27219: The function g_bytes_new has an integer overflow on 64-bit platforms due to an implicit cast from 64 bits to 32 bits. The overflow could potentially lead to memory corruption.	S1600E S100
2024-11-21	libglib2.0-0	CVE-2024-52533 CVE-2024-34397 CVE-	• Non-maintainer upload by the ELTS Team. • CVE-2024-52533: SOCKS4a proxy buffer overflow	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		2023-29499 CVE-2023-32611 CVE-2023-32665 CVE-2021-3800 CVE-2021-28153 CVE-2021-27218 CVE-2021-27219	• Non-maintainer upload the ELTS team. • Fix CVE-2024-34397: Alicia Boya Garcia reported that the GDBus signal subscriptions in the GLib library are prone to a spoofing vulnerability. A local attacker can take advantage of this flaw to cause a GDBus-based client to behave incorrectly, with an application-dependent impact. • Non-maintainer upload by the ELTS Team • Add debian/salsa-ci.yml using lts-team/pipeline for jessie • CVE-2023-29499: GVariant deserialization fails to validate that the input conforms to the expected format, leading to denial of service. • CVE-2023-32611: GVariant deserialization is vulnerable to a slowdown issue where a crafted GVariant can cause excessive processing, leading to denial of service. • CVE-2023-32665: GVariant deserialization is vulnerable to an exponential blowup issue where a crafted GVariant can cause excessive processing, leading to denial of service. • CVE-2021-3800: information leak using CHARSETALIASDIR envvar. • Non-maintainer upload by the ELTS team. • Fix CVE-2021-28153: When g_file_replace() is used with G_FILE_CREATE_REPLACE_DESTINATION to replace a path that is a dangling symlink, it incorrectly also creates the target of the symlink as an empty file, which could conceivably have security relevance if the symlink is attacker-controlled. (If the path is a symlink to a file that already exists, then the contents of that file correctly remain unchanged.) • Fix CVE-2021-27218: If g_byte_array_new_take() was called with a buffer of 4GB or more on a 64-bit platform, the length would be truncated modulo 2**32, causing unintended length truncation. • Fix CVE-2021-27219: The function g_bytes_new has an integer overflow on 64-bit platforms due to an implicit cast from 64 bits to 32 bits. The overflow could potentially lead to memory corruption.	
2024-11-28	libssl1.0.0	CVE-2023-5678 CVE-2024-0727 CVE-	• Non-maintainer upload by the ELTS Team. • Backport upstream fixes for	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		2023-0464 CVE-2023-0465 CVE-2023-0466 CVE-2023-2650 CVE-2023-3446 CVE-2023-0215 CVE-2023-0286 CVE-2022-2068 CVE-2022-2068 CVE-2022-1292 CVE-2022-0778 CVE-2021-3712	○ CVE-2023-5678 (denial of service w/ excessively long X9.42 DH keys) ○ CVE-2024-0727 (denial of service on null field in PKCS12 file) • Non-maintainer upload by the ELTS Team. • CVE-2023-0464 (Excessive Resource Usage Verifying X.509 Policy Constraints) • CVE-2023-0465 (invalid certificate policies in leaf certificates are silently ignored). • CVE-2023-0466 (Certificate policy check not enabled). • CVE-2023-2650 (Possible DoS translating ASN.1 object identifiers). • CVE-2023-3446 (Denial of service when checking DH keys or parameters). • Update expired test certificates. • Non-maintainer upload by the ELTS Team. • CVE-2023-0215 (Use-after-free following BIO_new_NDEF). • CVE-2023-0286 (X.400 address type confusion in X.509 GeneralName). • Non-maintainer upload by the ELTS Team. • Apply various upstream patches to c_rehash for the following fix. • CVE-2022-2068: command injection in c_rehash. • Apply c_rehash-compat.patch at the end, and update for the changes in CVE-2022-2068. Also update patch for CVE-2022-1292. • rehash-crt.patch: dropped. It’s partially superseded by the above changes (handling of extra extensions). The other part, supporting DER files, is obsolete and removed in later releases, and has the potential of suffering from the issue we’re fixing here (command injection via filenames), so be safe and drop it. • Non-maintainer upload by the ELTS Team.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• CVE-2022-1292: Do not use shell to invoke openssl in c_rehash. • Non-maintainer upload by the ELTS team. • CVE-2022-0778: infinite loop in BN_mod_sqrt. • Non-maintainer upload by the ELTS Team. • CVE-2021-3712 Read buffer overruns processing ASN.1 strings • Non-maintainer upload by the ELTS Security Team. • Fix verification error with alternate chains. Addresses issue with Let's Encrypt certificates starting 2021-10-01. https://lists.debian.org/debian-lts/2021/09/msg00008.html https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=961889	
2024-11-28	openssl	CVE-2023-5678 CVE-2024-0727 CVE-2023-0464 CVE-2023-0465 CVE-2023-0466 CVE-2023-2650 CVE-2023-3446 CVE-2023-0215 CVE-2023-0286 CVE-2022-2068 CVE-2022-2068 CVE-2022-1292 CVE-	• Non-maintainer upload by the ELTS Team. • Backport upstream fixes for ○ CVE-2023-5678 (denial of service w/ excessively long X9.42 DH keys) ○ CVE-2024-0727 (denial of service on null field in PKCS12 file) • Non-maintainer upload by the ELTS Team. • CVE-2023-0464 (Excessive Resource Usage Verifying X.509 Policy Constraints) • CVE-2023-0465 (invalid certificate policies in leaf certificates are silently ignored). • CVE-2023-0466 (Certificate policy check not enabled). • CVE-2023-2650 (Possible DoS translating ASN.1 object identifiers). • CVE-2023-3446 (Denial of service when checking DH keys or parameters). • Update expired test certificates.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		2022-0778 CVE-2021-3712	- Non-maintainer upload by the ELTS Team. - CVE-2023-0215 (Use-after-free following BIO_new_NDEF). - CVE-2023-0286 (X.400 address type confusion in X.509 GeneralName). - Non-maintainer upload by the ELTS Team. - Apply various upstream patches to c_rehash for the following fix. - CVE-2022-2068: command injection in c_rehash. - Apply c_rehash-compat.patch at the end, and update for the changes in CVE-2022-2068. Also update patch for CVE-2022-1292. - rehash-crt.patch: dropped. It's partially superseded by the above changes (handling of extra extensions). The other part, supporting DER files, is obsolete and removed in later releases, and has the potential of suffering from the issue we're fixing here (command injection via filenames), so be safe and drop it. - Non-maintainer upload by the ELTS Team. - CVE-2022-1292: Do not use shell to invoke openssl in c_rehash. - Non-maintainer upload by the ELTS team. - CVE-2022-0778: infinite loop in BN_mod_sqrt. - Non-maintainer upload by the ELTS Team. - CVE-2021-3712 Read buffer overruns processing ASN.1 strings - Non-maintainer upload by the ELTS Security Team. - Fix verification error with alternate chains. Addresses issue with Let's Encrypt certificates starting 2021-10-01. https://lists.debian.org/debian-lts/2021/09/msg00008.html https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=961889	
2024-12-08	libavahi-client3	CVE-2023-38469 CVE-2023-38470	- Non-maintainer upload by the ELTS Team. - CVE-2023-38469: Reachable assertion in avahi_dns_packet_append_record	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		CVE-2023-38471 CVE-2023-38472 CVE-2023-38473 CVE-2023-1981 CVE-2023-1981 CVE-2021-3468 CVE-2021-26720	• CVE-2023-38470: Reachable assertion in avahi_escape_label • CVE-2023-38471: Reachable assertion in dbus_set_host_name • CVE-2023-38472: Reachable assertion in avahi_rdata_parse • CVE-2023-38473: Reachable assertion in avahi_alternative_host_name • Fixed a GetAlternativeServiceName regression introduced by the CVE-2023-1981 fix in 0.6.31-5+deb8u2. • Non-maintainer upload by the Debian ELTS security team. • CVE-2023-1981: Fix an local Denial of Service (DoS) vulnerability where the avahi-daemon process could have been crashed over the DBus message bus. • Non-maintainer upload by the ELTS team. • Fix CVE-2021-3468: The event used to signal the termination of the client connection on the avahi Unix socket is not correctly handled in the client_work function, allowing a local attacker to trigger an infinite loop. • Fix CVE-2021-26720: avahi-daemon-check-dns.sh in the Debian avahi package is executed as root via /etc/network/if-up.d/avahi-daemon, and allows a local attacker to cause a denial of service or create arbitrary empty files via a symlink attack on files under /run/avahi-daemon. avahi-daemon: Depend on sudo in order to drop the root privileges.	
2024-12-08	libavahi-common3	CVE-2023-38469 CVE-2023-38470 CVE-2023-38471 CVE-2023-38472 CVE-2023-38473 CVE-2023-1981 CVE-2023-1981	• Non-maintainer upload by the ELTS Team. • CVE-2023-38469: Reachable assertion in avahi_dns_packet_append_record • CVE-2023-38470: Reachable assertion in avahi_escape_label • CVE-2023-38471: Reachable assertion in dbus_set_host_name • CVE-2023-38472: Reachable assertion in avahi_rdata_parse • CVE-2023-38473: Reachable assertion in avahi_alternative_host_name	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		CVE-2021-3468 CVE-2021-26720	- Fixed a GetAlternativeServiceName regression introduced by the CVE-2023-1981 fix in 0.6.31-5+deb8u2. - Non-maintainer upload by the Debian ELTS security team. - CVE-2023-1981: Fix an local Denial of Service (DoS) vulnerability where the avahi-daemon process could have been crashed over the DBus message bus. - Non-maintainer upload by the ELTS team. - Fix CVE-2021-3468: The event used to signal the termination of the client connection on the avahi Unix socket is not correctly handled in the client_work function, allowing a local attacker to trigger an infinite loop. - Fix CVE-2021-26720: avahi-daemon-check-dns.sh in the Debian avahi package is executed as root via /etc/network/if-up.d/avahi-daemon, and allows a local attacker to cause a denial of service or create arbitrary empty files via a symlink attack on files under /run/avahi-daemon. avahi-daemon: Depend on sudo in order to drop the root privileges.	
2024-12-08	libavahi-common-data	CVE-2023-38469 CVE-2023-38470 CVE-2023-38471 CVE-2023-38472 CVE-2023-38473 CVE-2023-1981 CVE-2023-1981 CVE-2021-3468 CVE-2021-26720	- Non-maintainer upload by the ELTS Team. - CVE-2023-38469: Reachable assertion in avahi_dns_packet_append_record - CVE-2023-38470: Reachable assertion in avahi_escape_label - CVE-2023-38471: Reachable assertion in dbus_set_host_name - CVE-2023-38472: Reachable assertion in avahi_rdata_parse - CVE-2023-38473: Reachable assertion in avahi_alternative_host_name - Fixed a GetAlternativeServiceName regression introduced by the CVE-2023-1981 fix in 0.6.31-5+deb8u2. - Non-maintainer upload by the Debian ELTS security team. - CVE-2023-1981: Fix an local Denial of Service (DoS) vulnerability where the avahi-daemon process could have been crashed over the DBus message bus.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Non-maintainer upload by the ELTS team. • Fix CVE-2021-3468: The event used to signal the termination of the client connection on the avahi Unix socket is not correctly handled in the client_work function, allowing a local attacker to trigger an infinite loop. • Fix CVE-2021-26720: avahi-daemon-check-dns.sh in the Debian avahi package is executed as root via /etc/network/if-up.d/avahi-daemon, and allows a local attacker to cause a denial of service or create arbitrary empty files via a symlink attack on files under /run/avahi-daemon. avahi-daemon: Depend on sudo in order to drop the root privileges.	
2025-01-17	rsync	CVE-2024-12087 CVE-2024-12085 CVE-2024-12086 CVE-2024-12087 CVE-2024-12088 CVE-2024-12747	• Non-maintainer upload by the ELTS Team. • fix for upstream regression of CVE-2024-12087 FLAG_GOT_DIR_FLIST collission with FLAG_HLINKED • fix use-after-free in generator • Non-maintainer upload by the ELTS Team. • CVE-2024-12085 prevent information leak off the stack • CVE-2024-12086 ○ refuse fuzzy options when fuzzy not selected ○ added secure_relative_open() ○ receiver: use secure_relative_open() for basis file ○ disallow ../ elements in relpath for secure_relative_open • CVE-2024-12087 ○ Refuse a duplicate dirlist. ○ range check dir_ndx before use • CVE-2024-12088 make --safe-links stricter • CVE-2024-12747 fixed symlink race condition in sender	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
2025-01-20	libtiff5	CVE-2024-7006 CVE-2023-52356 CVE-2023-25433 CVE-2023-52356 CVE-2023-3576 CVE-2023-2908 CVE-2023-3316 CVE-2023-3618 CVE-2023-25433 CVE-2023-26965 CVE-2023-26966 CVE-2023-38288 CVE-2023-38289 CVE-2023-0795 CVE-2023-0799 CVE-2023-0804 CVE-2022-0865 CVE-2022-0909 CVE-2022-2057 CVE-2022-3570 CVE-2022-	• Non-maintainer upload by the ELTS Team. • CVE-2024-7006: NULL pointer dereference in TIFFReadDirectory/TIFFReadCustomDirectory • Fixed a bug in the CVE-2023-52356 fix. • Added a missing part of the CVE-2023-25433 fix. • Non-maintainer upload by the ELTS Team. • CVE-2023-52356 A segment fault could be triggered by passing a crafted tiff file to the TIFFReadRGBATileExt() API • CVE-2023-3576 A memory leak flaw was found in Libtiff's tiffcrop utility. • Non-maintainer upload by the ELTS Security Team. • CVE-2023-2908: NULL pointer dereference in tif_dir.c • CVE-2023-3316: NULL pointer dereference in TIFFClose() • CVE-2023-3618: Buffer overflow in tiffcrop • CVE-2023-25433: Buffer overflow in tiffcrop • CVE-2023-26965: Use after free in tiffcrop • CVE-2023-26966: Buffer overflow in uv_encode() • CVE-2023-38288: Integer overflow in tiffcp • CVE-2023-38289: Integer overflow in raw2tiff • Non-maintainer upload by the ELTS team. • Fix CVE-2023-0795, CVE-2023-0796, CVE-2023-0797, CVE-2023-0798, CVE-2023-0799, CVE-2023-0800, CVE-2023-0801, CVE-2023-0802, CVE-2023-0803, CVE-2023-0804. Several flaws were found in tiffcrop, a program distributed by tiff, a library and tools providing support for the Tag Image File Format (TIFF). A specially crafted tiff file can lead to an out-of-bounds write or read resulting in a denial of service.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		3627 CVE-2020-19144 CVE-2020-19131	• Non-maintainer upload by the ELTS team. • Fix CVE-2022-0865, CVE-2022-0891, CVE-2022-0907, CVE-2022-0908, CVE-2022-0909, CVE-2022-0924, CVE-2022-1355, CVE-2022-2056, CVE-2022-2057, CVE-2022-2058, CVE-2022-2867, CVE-2022-2868, CVE-2022-2869, CVE-2022-3570, CVE-2022-3597, CVE-2022-3598, CVE-2022-3599, CVE-2022-3626, CVE-2022-3627, CVE-2022-3970, CVE-2022-34526 and CVE-2022-48281. Multiple vulnerabilities were found in tiff, a library and tools providing support for the Tag Image File Format (TIFF), leading to denial of service (DoS) and possibly local code execution. • Update libtiff5.symbols and add new symbols _TIFFClampDoubleToUInt32@LIBTIFF_4.0, _TIFFMultiplySSize@LIBTIFF_4.0 and _TIFFCastUInt64ToSSize@LIBTIFF_4.0. • Non-maintainer upload by the ELTS Team. • Non-maintainer upload by the ELTS team. • Add patch so that LogLuvSetupEncode() error must return 0. (Fixes: CVE-2020-19144) • Add patch to fix invertImage() for bps 2 and 4. (Fixes: CVE-2020-19131)	
2025-02-23	krb5-locales	CVE-2024-26462 CVE-2024-26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371 CVE-2023-36054 CVE-2022-42898	• Non Maintainer upload by LTS team • Fixes CVE-2024-26462 A memory leak vulnerability was found in /krb5/src/kdc/ndr.c. • Non-maintainer upload by the ELTS Team. • CVE-2024-26458: Memory leak in xmt_rmtcallres() • CVE-2024-26461: Memory leak in gss_krb5int_make_seal_token_v3() • CVE-2024-37370: GSS wrap token Extra Count field manipulation • CVE-2024-37371: Invalid GSS memory reads with manipulated tokens • Non-maintainer upload by the ELTS Security Team. • CVE-2023-36054: Freeing of uninitialized pointer in kadm_rpc_xdr.c	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
			- Non-maintainer upload by the ELTS Team. - CVE-2022-42898: Prevent integer overflows in PAC parsing; potentially critical for 32-bit KDCs or when cross-realm acts maliciously.	
2025-02-23	libk5crypto3	CVE-2024-26462 CVE-2024-26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371 CVE-2023-36054 CVE-2022-42898	- Non Maintainer upload by LTS team - Fixes CVE-2024-26462 A memory leak vulnerability was found in /krb5/src/kdc/ndr.c. - Non-maintainer upload by the ELTS Team. - CVE-2024-26458: Memory leak in xmt_rmtcallres() - CVE-2024-26461: Memory leak in gss_krb5int_make_seal_token_v3() - CVE-2024-37370: GSS wrap token Extra Count field manipulation - CVE-2024-37371: Invalid GSS memory reads with manipulated tokens - Non-maintainer upload by the ELTS Security Team. - CVE-2023-36054: Freeing of uninitialized pointer in kadm_rpc_xdr.c - Non-maintainer upload by the ELTS Team. - CVE-2022-42898: Prevent integer overflows in PAC parsing; potentially critical for 32-bit KDCs or when cross-realm acts maliciously.	M400 M410 R100E R100NA S1600E S100
2025-02-23	libgssapi-krb5-2	CVE-2024-26462 CVE-2024-26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371 CVE-2023-	- Non Maintainer upload by LTS team - Fixes CVE-2024-26462 A memory leak vulnerability was found in /krb5/src/kdc/ndr.c. - Non-maintainer upload by the ELTS Team. - CVE-2024-26458: Memory leak in xmt_rmtcallres() - CVE-2024-26461: Memory leak in gss_krb5int_make_seal_token_v3()	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		36054 CVE-2022-42898	- CVE-2024-37370: GSS wrap token Extra Count field manipulation - CVE-2024-37371: Invalid GSS memory reads with manipulated tokens - Non-maintainer upload by the ELTS Security Team. - CVE-2023-36054: Freeing of uninitialized pointer in kadm_rpc_xdr.c - Non-maintainer upload by the ELTS Team. - CVE-2022-42898: Prevent integer overflows in PAC parsing; potentially critical for 32-bit KDCs or when cross-realm acts maliciously.	
2025-02-23	libkrb5-3	CVE-2024-26462 CVE-2024-26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371 CVE-2023-36054 CVE-2022-42898	- Non Maintainer upload by LTS team - Fixes CVE-2024-26462 A memory leak vulnerability was found in /krb5/src/kdc/ndr.c. - Non-maintainer upload by the ELTS Team. - CVE-2024-26458: Memory leak in xmt_rmtcallres() - CVE-2024-26461: Memory leak in gss_krb5int_make_seal_token_v3() - CVE-2024-37370: GSS wrap token Extra Count field manipulation - CVE-2024-37371: Invalid GSS memory reads with manipulated tokens - Non-maintainer upload by the ELTS Security Team. - CVE-2023-36054: Freeing of uninitialized pointer in kadm_rpc_xdr.c - Non-maintainer upload by the ELTS Team. - CVE-2022-42898: Prevent integer overflows in PAC parsing; potentially critical for 32-bit KDCs or when cross-realm acts maliciously.	M400 M410 R100E R100NA S1600E S100
2025-02-23	libkrb5support0	CVE-2024-26462 CVE-2024-	- Non Maintainer upload by LTS team	M400 M410 R100E R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
		26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371 CVE-2023-36054 CVE-2022-42898	• Fixes CVE-2024-26462 A memory leak vulnerability was found in /krb5/src/kdc/ndr.c. • Non-maintainer upload by the ELTS Team. • CVE-2024-26458: Memory leak in xmt_rmtcallres() • CVE-2024-26461: Memory leak in gss_krb5int_make_seal_token_v3() • CVE-2024-37370: GSS wrap token Extra Count field manipulation • CVE-2024-37371: Invalid GSS memory reads with manipulated tokens • Non-maintainer upload by the ELTS Security Team. • CVE-2023-36054: Freeing of uninitialized pointer in kadm_rpc_xdr.c • Non-maintainer upload by the ELTS Team. • CVE-2022-42898: Prevent integer overflows in PAC parsing; potentially critical for 32-bit KDCs or when cross-realm acts maliciously.	S1600E S100
2025-02-27	libtasn1-6	CVE-2024-12133 CVE-2021-46848	• Non-maintainer upload by the ELTS Team. • Fix CVE-2024-12133: Potential DoS while parsing a certificate containing numerous SEQUENCE OF or SET OF elements. • Non-maintainer upload by the ELTS Team. • CVE-2021-46848 Fix an off-by-one array size issue that affected the asn1_encode_simple_der function. • Move texinfo to Build-Depends to fix "any"-style build.	M400 M410 R100E R100NA S1600E S100
2025-03-11	python2.7-minimal	CVE-2023-27043 CVE-2024-6232 CVE-2024-6923 CVE-2024-	• Non-maintainer upload by the ELTS team. • Fix CVE-2023-27043: The email module of Python incorrectly parses e-mail addresses that contain a special character. The wrong portion of an RFC2822 header is identified as the value of the addr-spec. In some applications, an attacker can bypass a protection mechanism in which application access is granted only after verifying receipt of e-mail to a	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		7592 CVE-2024-5642 CVE-2024-5535 CVE-2024-11168 CVE-2025-0938 CVE-2024-0450 CVE-2021-23336 CVE-2022-0391 CVE-2022-48560 CVE-2022-48565 CVE-2022-48566 CVE-2023-24329 CVE-2023-40217 CVE-2015-20107 CVE-2020-8492 CVE-2020-26116 CVE-2021-3733 CVE-2021-3737 CVE-2022-45061 CVE-2021-3177 CVE-2019-16935 CVE-	specific domain (e.g., only @company.example.com addresses may be used for signup). • Fix CVE-2024-6232: Regular expressions that allowed excessive backtracking during tarfile.TarFile header parsing are vulnerable to ReDoS via specifically-crafted tar archives. • Fix CVE-2024-6923: The email module didn't properly quote newlines for email headers when serializing an email message allowing for header injection when an email is serialized. • Fix CVE-2024-7592: When parsing cookies that contained backslashes for quoted characters in the cookie value, the parser would use an algorithm with quadratic complexity, resulting in excess CPU resources being used while parsing the value. • Testsuite fixes: ○ test_signal: install procps (for missing /bin/kill) • Avoid Salsa-CI timeouts: Always run the testsuite subset that buildds use. Disable PGO on Salsa-CI. • CVE-2024-5642: CPython doesn't disallow configuring an empty list ("[]") for SSLContext.set_npn_protocols() which is an invalid value for the underlying OpenSSL API. This results in a buffer over-read when NPN is used (see CVE-2024-5535 for OpenSSL). This vulnerability is of low severity due to NPN being not widely used and specifying an empty list likely being uncommon in-practice (typically a protocol name would be configured). • CVE-2024-11168: The urllib.parse.urlsplit() and urlparse() functions improperly validated bracketed hosts ([]), allowing hosts that weren't IPv6 or IPvFuture. This behavior was not conformant to RFC 3986 and potentially enabled SSRF if a URL is processed by more than one URL parser. • CVE-2025-0938: urllib.parse.urlsplit and urlparse accepted domain names that included square brackets which isn't valid according to RFC 1. Square brackets are only meant to be used as delimiters for specifying IPv6 and IPvFuture hosts in URLs. This could result in differential parsing across the Python URL parser and other specification-compliant URL parsers. • Testsuite fixes: ○ test_os: conditionally disable fsync/fdatasync tests under eatmydata |	

Date	Package	CVE(s)	Synopsys	Hardware Version
		2021-4189 CVE-2019-16935 CVE-2021-4189 CVE-2021-3177	○ test_ssl, test_httplib: fix tests relying on old SSL protocol ○ test_ssl: enable and fix tests for CVE 2023-40217 ○ test_cookie: backport test cases for CVE 2024-7592 • Salsa-CI fixes: ○ debian/salsa-ci.yml: rename and tidy Salsa-CI configuration ○ Depend on netbase in DEP-8 tests (for /etc/services) ○ Fix test-build-all: create stamps when generating doc • Non-maintainer upload by the ELTS Team. • CVE-2024-0450: quoted-overlap zipbomb DoS • Non-maintainer upload by the LTS Team. • Add testsuite-fix-with-expat.diff: Fix autopkgtests with updated expat. • Fix issue9189.diff: Update test suite to match behaviour change. • Fix CVE-2021-23336.diff: Delete diagnostic output breaking test acceptance. • autopkgtest: Mark distutils as non-failing. • Add testsuite-skip-zipfile-issue17753.diff: Skip failing tests. • Add CVE-2022-0391.diff: Make urlsplit robust against newlines • Add CVE-2022-48560.diff: Fix use-after-free in heapq module. • Add CVE-2022-48565.diff: Reject entities declarations while parsing XML plists. • Add CVE-2022-48566.diff: Make constant time comparison more constant-time. • Add CVE-2023-24329.diff: More WHATWG-compatible URL parsing	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Add CVE-2023-40217.diff: Prevent reading unauthenticated data on a SSLSocket • Non-maintainer upload by the ELTS Security Team. • Update self-signed.pythontest.net SSL certificate in testsuite (fixes test_httplib test suite) • Update test certificates and keys (fixes test_ssl test suite) • Update external test servers (fixes test_urllib2net and test_ssl test suites) • Drop CVE 2019-9740/2019-9947 patch which attempted to fix an issue introduced later in v2.7.14 and didn't pass its own test cases • Replace CVE 2019-10160 fix with buster's more complete one; fix test_urlparse:test_urlsplit_normalization test case • CVE-2015-20107: the mailcap module does not add escape characters into commands discovered in the system mailcap file. This may allow attackers to inject shell commands into applications that call mailcap.findmatch with untrusted input (if they lack validation of user-provided filenames or arguments). • CVE-2020-8492: Python allows an HTTP server to conduct Regular Expression Denial of Service (ReDoS) attacks against a client because of urllib.request.AbstractBasicAuthHandler catastrophic backtracking. • CVE-2020-26116: http.client allows CRLF injection if the attacker controls the HTTP request method, as demonstrated by inserting CR and LF control characters in the first argument of HTTPConnection.request. • CVE-2021-3733: There's a flaw in urllib's AbstractBasicAuthHandler class. An attacker who controls a malicious HTTP server that an HTTP client (such as web browser) connects to, could trigger a Regular Expression Denial of Service (ReDOS) during an authentication request with a specially crafted payload that is sent by the server to the client. • CVE-2021-3737: An improperly handled HTTP response in the HTTP client code of python may allow a remote attacker, who controls the HTTP server, to make the client script enter an infinite loop, consuming CPU time. • CVE-2022-45061: An unnecessary quadratic algorithm exists in one path when processing some inputs to the IDNA (RFC 3490) decoder, such that a crafted, unreasonably long name being presented to the decoder could lead to a CPU denial of service.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• d/p/CVE-2021-3177: Use PyString_FromFormat over PyUnicode_FromFormat. • d/p/CVE-2019-16935: Add patch to avoid race condition in server setup. • d/p/CVE-2021-4189: Refactor patch as per v2.7.9’s codebase. • Non-maintainer upload by the ELTS team. • CVE-2019-16935: Escape the server title of DocXMLRPCServer. • CVE-2021-4189: Make ftplib not trust the PASV response. • CVE-2021-3177: Replace snprintf with Python unicode formatting in ctypes param reprs.	
2025-03-11	python2.7	CVE-2023-27043 CVE-2024-6232 CVE-2024-6923 CVE-2024-7592 CVE-2024-5642 CVE-2024-5535 CVE-2024-11168 CVE-2025-0938 CVE-2024-0450 CVE-2021-23336 CVE-2022-0391 CVE-2022-48560 CVE-	• Non-maintainer upload by the ELTS team. • Fix CVE-2023-27043: The email module of Python incorrectly parses e-mail addresses that contain a special character. The wrong portion of an RFC2822 header is identified as the value of the addr-spec. In some applications, an attacker can bypass a protection mechanism in which application access is granted only after verifying receipt of e-mail to a specific domain (e.g., only @company.example.com addresses may be used for signup). • Fix CVE-2024-6232: Regular expressions that allowed excessive backtracking during tarfile.TarFile header parsing are vulnerable to ReDoS via specifically-crafted tar archives. • Fix CVE-2024-6923: The email module didn’t properly quote newlines for email headers when serializing an email message allowing for header injection when an email is serialized. • Fix CVE-2024-7592: When parsing cookies that contained backslashes for quoted characters in the cookie value, the parser would use an algorithm with quadratic complexity, resulting in excess CPU resources being used while parsing the value. • Testsuite fixes: ○ test_signal: install procps (for missing /bin/kill) • Avoid Salsa-CI timeouts: Always run the testsuite subset that buildds use. Disable PGO on Salsa-CI.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		2022-48565 CVE-2022-48566 CVE-2023-24329 CVE-2023-40217 CVE-2015-20107 CVE-2020-8492 CVE-2020-26116 CVE-2021-3733 CVE-2021-3737 CVE-2022-45061 CVE-2021-3177 CVE-2019-16935 CVE-2021-4189 CVE-2019-16935 CVE-2021-4189 CVE-2021-3177	• CVE-2024-5642: CPython doesn’t disallow configuring an empty list ("[]") for SSLContext.set_npn_protocols() which is an invalid value for the underlying OpenSSL API. This results in a buffer over-read when NPN is used (see CVE-2024-5535 for OpenSSL). This vulnerability is of low severity due to NPN being not widely used and specifying an empty list likely being uncommon in-practice (typically a protocol name would be configured). • CVE-2024-11168: The urllib.parse.urlsplit() and urlparse() functions improperly validated bracketed hosts ([]), allowing hosts that weren’t IPv6 or IPvFuture. This behavior was not conformant to RFC 3986 and potentially enabled SSRF if a URL is processed by more than one URL parser. • CVE-2025-0938: urllib.parse.urlsplit and urlparse accepted domain names that included square brackets which isn’t valid according to RFC 1. Square brackets are only meant to be used as delimiters for specifying IPv6 and IPvFuture hosts in URLs. This could result in differential parsing across the Python URL parser and other specification-compliant URL parsers. • Testsuite fixes: ○ test_os: conditionally disable fsync/fdatasync tests under eatmydata | ○ test_ssl, test_httplib: fix tests relying on old SSL protocol ○ test_ssl: enable and fix tests for CVE 2023-40217 ○ test_cookie: backport test cases for CVE 2024-7592 • Salsa-CI fixes: ○ debian/salsa-ci.yml: rename and tidy Salsa-CI configuration ○ Depend on netbase in DEP-8 tests (for /etc/services) ○ Fix test-build-all: create stamps when generating doc • Non-maintainer upload by the ELTS Team. • CVE-2024-0450: quoted-overlap zipbomb DoS • Non-maintainer upload by the LTS Team.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- Add testsuite-fix-with-expat.diff: Fix autopkgtests with updated expat. - Fix issue9189.diff: Update test suite to match behaviour change. - Fix CVE-2021-23336.diff: Delete diagnostic output breaking test acceptance. - autopkgtest: Mark distutils as non-failing. - Add testsuite-skip-zipfile-issue17753.diff: Skip failing tests. - Add CVE-2022-0391.diff: Make urlsplit robust against newlines - Add CVE-2022-48560.diff: Fix use-after-free in heapq module. - Add CVE-2022-48565.diff: Reject entities declarations while parsing XML plists. - Add CVE-2022-48566.diff: Make constant time comparison more constant-time. - Add CVE-2023-24329.diff: More WHATWG-compatible URL parsing - Add CVE-2023-40217.diff: Prevent reading unauthenticated data on a SSLSocket - Non-maintainer upload by the ELTS Security Team. - Update self-signed.pythontest.net SSL certificate in testsuite (fixes test_httplib test suite) - Update test certificates and keys (fixes test_ssl test suite) - Update external test servers (fixes test_urllib2net and test_ssl test suites) - Drop CVE 2019-9740/2019-9947 patch which attempted to fix an issue introduced later in v2.7.14 and didn't pass its own test cases - Replace CVE 2019-10160 fix with buster's more complete one; fix test_urlparse:test_urlsplit_normalization test case - CVE-2015-20107: the mailcap module does not add escape characters into commands discovered in the system mailcap file. This may allow attackers to inject shell commands into applications that call	

Date	Package	CVE(s)	Synopsys	Hardware Version
			mailcap.findmatch with untrusted input (if they lack validation of user-provided filenames or arguments). • CVE-2020-8492: Python allows an HTTP server to conduct Regular Expression Denial of Service (ReDoS) attacks against a client because of urllib.request.AbstractBasicAuthHandler catastrophic backtracking. • CVE-2020-26116: http.client allows CRLF injection if the attacker controls the HTTP request method, as demonstrated by inserting CR and LF control characters in the first argument of HTTPConnection.request. • CVE-2021-3733: There's a flaw in urllib's AbstractBasicAuthHandler class. An attacker who controls a malicious HTTP server that an HTTP client (such as web browser) connects to, could trigger a Regular Expression Denial of Service (ReDOS) during an authentication request with a specially crafted payload that is sent by the server to the client. • CVE-2021-3737: An improperly handled HTTP response in the HTTP client code of python may allow a remote attacker, who controls the HTTP server, to make the client script enter an infinite loop, consuming CPU time. • CVE-2022-45061: An unnecessary quadratic algorithm exists in one path when processing some inputs to the IDNA (RFC 3490) decoder, such that a crafted, unreasonably long name being presented to the decoder could lead to a CPU denial of service. • d/p/CVE-2021-3177: Use PyString_FromFormat over PyUnicode_FromFormat. • d/p/CVE-2019-16935: Add patch to avoid race condition in server setup. • d/p/CVE-2021-4189: Refactor patch as per v2.7.9's codebase. • Non-maintainer upload by the ELTS team. • CVE-2019-16935: Escape the server title of DocXMLRPCServer. • CVE-2021-4189: Make ftplib not trust the PASV response. • CVE-2021-3177: Replace snprintf with Python unicode formatting in ctypes param reprs.	
2025-03-11	libpython2.7-minimal	CVE-2023-27043 CVE-	• Non-maintainer upload by the ELTS team.	M400 M410 R100E R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
		2024-6232 CVE-2024-6923 CVE-2024-7592 CVE-2024-5642 CVE-2024-5535 CVE-2024-11168 CVE-2025-0938 CVE-2024-0450 CVE-2021-23336 CVE-2022-0391 CVE-2022-48560 CVE-2022-48565 CVE-2022-48566 CVE-2023-24329 CVE-2023-40217 CVE-2015-20107 CVE-2020-8492 CVE-2020-26116 CVE-2021-3733 CVE-2021-3737 CVE-2022-45061	• Fix CVE-2023-27043: The email module of Python incorrectly parses e-mail addresses that contain a special character. The wrong portion of an RFC2822 header is identified as the value of the addr-spec. In some applications, an attacker can bypass a protection mechanism in which application access is granted only after verifying receipt of e-mail to a specific domain (e.g., only @company.example.com addresses may be used for signup). • Fix CVE-2024-6232: Regular expressions that allowed excessive backtracking during tarfile.TarFile header parsing are vulnerable to ReDoS via specifically-crafted tar archives. • Fix CVE-2024-6923: The email module didn’t properly quote newlines for email headers when serializing an email message allowing for header injection when an email is serialized. • Fix CVE-2024-7592: When parsing cookies that contained backslashes for quoted characters in the cookie value, the parser would use an algorithm with quadratic complexity, resulting in excess CPU resources being used while parsing the value. • Testsuite fixes: ○ test_signal: install procps (for missing /bin/kill) • Avoid Salsa-CI timeouts: Always run the testsuite subset that buildds use. Disable PGO on Salsa-CI. • CVE-2024-5642: CPython doesn’t disallow configuring an empty list ("[]") for SSLContext.set_npn_protocols() which is an invalid value for the underlying OpenSSL API. This results in a buffer over-read when NPN is used (see CVE-2024-5535 for OpenSSL). This vulnerability is of low severity due to NPN being not widely used and specifying an empty list likely being uncommon in-practice (typically a protocol name would be configured). • CVE-2024-11168: The urllib.parse.urlsplit() and urlparse() functions improperly validated bracketed hosts ([]), allowing hosts that weren’t IPv6 or IPvFuture. This behavior was not conformant to RFC 3986 and potentially enabled SSRF if a URL is processed by more than one URL parser. • CVE-2025-0938: urllib.parse.urlsplit and urlparse accepted domain names that included square brackets which isn’t valid according to RFC 1. Square brackets are only meant to be used as delimiters for specifying IPv6 and IPvFuture hosts in URLs. This could result in differential parsing across the Python URL parser and other specification-compliant URL parsers.	S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		CVE-2021-3177 CVE-2019-16935 CVE-2021-4189 CVE-2019-16935 CVE-2021-4189 CVE-2021-3177	• Testsuite fixes: ○ test_os: conditionally disable fsync/fdatasync tests under eatmydata | ○ test_ssl, test_httplib: fix tests relying on old SSL protocol ○ test_ssl: enable and fix tests for CVE 2023-40217 ○ test_cookie: backport test cases for CVE 2024-7592 • Salsa-CI fixes: ○ debian/salsa-ci.yml: rename and tidy Salsa-CI configuration ○ Depend on netbase in DEP-8 tests (for /etc/services) ○ Fix test-build-all: create stamps when generating doc • Non-maintainer upload by the ELTS Team. • CVE-2024-0450: quoted-overlap zipbomb DoS • Non-maintainer upload by the LTS Team. • Add testsuite-fix-with-expat.diff: Fix autopkgtests with updated expat. • Fix issue9189.diff: Update test suite to match behaviour change. • Fix CVE-2021-23336.diff: Delete diagnostic output breaking test acceptance. • autopkgtest: Mark distutils as non-failing. • Add testsuite-skip-zipfile-issue17753.diff: Skip failing tests. • Add CVE-2022-0391.diff: Make urlsplit robust against newlines • Add CVE-2022-48560.diff: Fix use-after-free in heapq module. • Add CVE-2022-48565.diff: Reject entities declarations while parsing XML plists.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Add CVE-2022-48566.diff: Make constant time comparison more constant-time. • Add CVE-2023-24329.diff: More WHATWG-compatible URL parsing • Add CVE-2023-40217.diff: Prevent reading unauthenticated data on a SSLSocket • Non-maintainer upload by the ELTS Security Team. • Update self-signed.pythontest.net SSL certificate in testsuite (fixes test_httplib test suite) • Update test certificates and keys (fixes test_ssl test suite) • Update external test servers (fixes test_urllib2net and test_ssl test suites) • Drop CVE 2019-9740/2019-9947 patch which attempted to fix an issue introduced later in v2.7.14 and didn’t pass its own test cases • Replace CVE 2019-10160 fix with buster’s more complete one; fix test_urlparse:test_urlsplit_normalization test case • CVE-2015-20107: the mailcap module does not add escape characters into commands discovered in the system mailcap file. This may allow attackers to inject shell commands into applications that call mailcap.findmatch with untrusted input (if they lack validation of user-provided filenames or arguments). • CVE-2020-8492: Python allows an HTTP server to conduct Regular Expression Denial of Service (ReDoS) attacks against a client because of urllib.request.AbstractBasicAuthHandler catastrophic backtracking. • CVE-2020-26116: http.client allows CRLF injection if the attacker controls the HTTP request method, as demonstrated by inserting CR and LF control characters in the first argument of HTTPConnection.request. • CVE-2021-3733: There’s a flaw in urllib’s AbstractBasicAuthHandler class. An attacker who controls a malicious HTTP server that an HTTP client (such as web browser) connects to, could trigger a Regular Expression Denial of Service (ReDOS) during an authentication request with a specially crafted payload that is sent by the server to the client. • CVE-2021-3737: An improperly handled HTTP response in the HTTP client code of python may allow a remote attacker, who controls the HTTP server, to make the client script enter an infinite loop, consuming CPU time.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- CVE-2022-45061: An unnecessary quadratic algorithm exists in one path when processing some inputs to the IDNA (RFC 3490) decoder, such that a crafted, unreasonably long name being presented to the decoder could lead to a CPU denial of service. - d/p/CVE-2021-3177: Use PyString_FromFormat over PyUnicode_FromFormat. - d/p/CVE-2019-16935: Add patch to avoid race condition in server setup. - d/p/CVE-2021-4189: Refactor patch as per v2.7.9's codebase. - Non-maintainer upload by the ELTS team. - CVE-2019-16935: Escape the server title of DocXMLRPCServer. - CVE-2021-4189: Make ftplib not trust the PASV response. - CVE-2021-3177: Replace snprintf with Python unicode formatting in ctypes param reprs.	
2025-03-15	libgnutls-deb0-28	CVE-2024-12243	- Non-maintainer upload by the ELTS Team. - d/control: Ensure that the package is built with nettle2, to avoid CVE 2021-4209. gnutls28 is only vulnerable when built with nettle3. - Fix CVE-2024-12243: Potential DoS while parsing a certificate containing numerous names or name constraints. - Non-maintainer upload by the ELTS Security Team. - Fix verification error with alternate chains. Addresses issue with Let's Encrypt certificates starting 2021-10-01. https://lists.debian.org/debian-lts/2021/09/msg00008.html	M400 M410 R100E R100NA S1600E S100
2025-03-15	libgnutls-openssl27	CVE-2024-12243	- Non-maintainer upload by the ELTS Team. - d/control: Ensure that the package is built with nettle2, to avoid CVE 2021-4209. gnutls28 is only vulnerable when built with nettle3. - Fix CVE-2024-12243: Potential DoS while parsing a certificate containing numerous names or name constraints.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Non-maintainer upload by the ELTS Security Team. • Fix verification error with alternate chains. Addresses issue with Let’s Encrypt certificates starting 2021-10-01. https://lists.debian.org/debian-lts/2021/09/msg00008.html	
2025-04-14	python-jinja2	CVE-2024-56326 CVE-2024-56326 CVE-2025-27516 CVE-2025-27516 CVE-2024-22195	• Non-maintainer upload by the ELTS team. • Fix CVE-2024-56326. An oversight in how the Jinja sandboxed environment detects calls to str.format allows an attacker that controls the content of a template to execute arbitrary Python code. ○ d/p/CVE-2024-56326.patch • Fix CVE-2025-27516. An oversight in how the Jinja sandboxed environment interacts with the |attr filter allows an attacker that controls the content of a template to execute arbitrary Python code. ○ d/p/CVE-2025-27516.patch • Non-maintainer upload by the ELTS team. • CVE-2024-22195: Fix an issue where it was possible to inject arbitrary HTML attributes into the rendered HTML via the "xmlattr" filter, potentially leading to a Cross-Site Scripting (XSS) attack. It may also have been possible to bypass attribute validation checks if they were blacklist-based.	M400 M410 R100E R100NA S1600E S100
2025-04-15	passwd	CVE-2023-4641 CVE-2023-29383 CVE-2017-12424 CVE-2017-12424 CVE-2018-7169 CVE-2018-7169	• Non-maintainer upload by the ELTS Security Team. • CVE-2023-4641: When asking for a new password, shadow-utils asks the password twice. If the password fails on the second attempt, shadow-utils fails in cleaning the buffer used to store the first entry. This may allow an attacker with enough access to retrieve the password from the memory. • CVE-2023-29383: It is possible to inject control characters into fields provided to the SUID program chfn (change finger). Although it is not possible to exploit this directly (e.g., adding a new user fails because \n is in the block list), it is possible to misrepresent the /etc/passwd file when viewed. • Non-maintainer upload by the ELTS team. • SECURITY UPDATE: Crash or buffer overflow	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ debian/patches/CVE-2017-12424.patch: fix buffer overflow if NULL line is present in db in lib/commonio.c. ○ CVE-2017-12424 • SECURITY UPDATE: Access to privileged information ○ debian/patches/CVE-2018-7169.patch: newgidmap: enforce setgroups=deny if self-mapping a group in src/newgidmap.c. ○ CVE-2018-7169	
2025-04-15	login	CVE-2023-4641 CVE-2023-29383 CVE-2017-12424 CVE-2017-12424 CVE-2018-7169 CVE-2018-7169	• Non-maintainer upload by the ELTS Security Team. • CVE-2023-4641: When asking for a new password, shadow-utils asks the password twice. If the password fails on the second attempt, shadow-utils fails in cleaning the buffer used to store the first entry. This may allow an attacker with enough access to retrieve the password from the memory. • CVE-2023-29383: It is possible to inject control characters into fields provided to the SUID program chfn (change finger). Although it is not possible to exploit this directly (e.g., adding a new user fails because \n is in the block list), it is possible to misrepresent the /etc/passwd file when viewed. • Non-maintainer upload by the ELTS team. • SECURITY UPDATE: Crash or buffer overflow ○ debian/patches/CVE-2017-12424.patch: fix buffer overflow if NULL line is present in db in lib/commonio.c. ○ CVE-2017-12424 • SECURITY UPDATE: Access to privileged information ○ debian/patches/CVE-2018-7169.patch: newgidmap: enforce setgroups=deny if self-mapping a group in src/newgidmap.c. ○ CVE-2018-7169	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
2025-04-20	wget	CVE-2024-38428	• Non-maintainer upload by the ELTS Team. • CVE-2024-38428: Mishandling of semicolons in the userinfo subcomponent of a URI	M400 M410 R100E R100NA S1600E S100
2025-04-27	libxml2	CVE-2025-32414 CVE-2025-32415 CVE-2022-49043 CVE-2024-56171 CVE-2025-24928 CVE-2025-27113 CVE-2016-9318 CVE-2017-16932 CVE-2023-39615 CVE-2023-45322 CVE-2024-25062 CVE-2022-2309 CVE-2023-28484 CVE-2023-29469 CVE-2017-5969 CVE-2017-5130 CVE-2022-40303 CVE-2022-40304	• Non-maintainer upload by the ELTS Team. • CVE-2025-32414 fix for out-of-bounds memory access in the Python API • CVE-2025-32415 fix for heap-buffer-overflow in xmlSchemaIDCFillNodeTables() • Non-maintainer upload by the ELTS Security Team. • Import upstream patches for ○ CVE-2022-49043 - Use after free ○ CVE-2024-56171 - Use after free ○ CVE-2025-24928 - Stack based buffer overflow ○ CVE-2025-27113 - NULL pointer dereference • Non-maintainer upload by the ELTS Security Team. • Backport patches from the last stretch upload: ○ CVE-2016-9318 - improve handling of context input_id ○ CVE-2017-16932 - infinite recursion in parameter entities • CVE-2023-39615 - Crash with XML_PARSE_SAX1 Parser option • CVE-2023-45322 - Use after free after memory allocation • CVE-2024-25062 - Use after free with DTD validation and XInclude expansion enabled • Non-maintainer upload by the ELTS Team.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		CVE-2022-29824 CVE-2022-23308	• CVE-2022-2309: Parser NULL pointer dereference • Non-maintainer upload by the ELTS Security Team. • Apply upstream patch for CVE-2023-28484: NULL dereference in xmlSchemaFixupComplexType. • Apply upstream patch for CVE-2023-29469 Hashing of empty dict strings wasn't deterministic. • Fix CVE-2017-5969 NULL pointer dereference in xmlDumpElementContent in recovery mode. • Add patches for CVE-2017-5130 An integer overflow possibly causing heap corruption. • Non-maintainer upload by the ELTS team. • Fix CVE-2022-40303: Parsing a XML document with the XML_PARSE_HUGE option enabled can result in an integer overflow because safety checks were missing in some functions. Also, the xmlParseEntityValue function didn't have any length limitation. • Fix CVE-2022-40304: When a reference cycle is detected in the XML entity cleanup function the XML entity data can be stored in a dictionary. In this case, the dictionary becomes corrupted resulting in logic errors, including memory errors like double free. • Non-maintainer upload by the ELTS team. • Fix CVE-2022-29824: Felix Wilhelm discovered that libxml2 did not correctly check for integer overflows or used wrong types for buffer sizes. This could result in out-of-bounds writes or other memory errors when working on large, multi-gigabyte buffers. • Non-maintainer upload by the ELTS Team. • CVE-2022-23308: Fix use-after-free of ID and IDREF attributes	
2025-05-20	vim-common	CVE-2023-4738 CVE-2024-22667 CVE-2024-43802	• Non-maintainer upload by the Security Team. • CVE-2023-4738: buffer-overflow in vim_regsub_both • CVE-2024-22667: stack-buffer-overflow in option callback functions	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsys	Hardware Version
		CVE-2024-47814 CVE-2023-4752 CVE-2023-4781 CVE-2023-5344 CVE-2022-4141 CVE-2022-1785 CVE-2022-2129 CVE-2022-2285 CVE-2022-3134 CVE-2022-1851 CVE-2021-3903 CVE-2022-0572 CVE-2022-1720 CVE-2022-1154 CVE-2021-3872 CVE-2021-3984 CVE-2022-0213 CVE-2022-0408 CVE-2021-3796	• CVE-2024-43802: heap-buffer-overflow in ins_typebuf • CVE-2024-47814: use-after-free when closing a buffer • Fix arch:all build • Non-maintainer upload by the ELTS Team. • CVE-2023-4752: Heap use after free in ins_compl_get_exp() • CVE-2023-4781: Heap buffer-overflow in vim_regsub_both() • CVE-2023-5344: Heap buffer-overflow in trunc_string() • Non-maintainer upload by the ELTS team. • Fix CVE-2022-4141, CVE-2023-0054, CVE-2023-1175, CVE-2023-2610: Multiple security vulnerabilities have been discovered in vim, an enhanced vi editor. Buffer overflows and out-of-bounds reads may lead to a denial-of-service (application crash) or other unspecified impact. • Non-maintainer upload by the ELTS team. • Fix CVE-2022-1785, CVE-2022-1897, CVE-2022-1942, CVE-2022-2000 CVE-2022-2129, CVE-2022-3235, CVE-2022-3256 • Non-maintainer upload by the ELTS team. • Fix CVE-2022-2285, CVE-2022-2304, CVE-2022-2946, CVE-2022-3099, CVE-2022-3134, CVE-2022-3234, CVE-2022-3324. • Multiple security vulnerabilities have been discovered in vim, an enhanced vi editor. Buffer overflows, out-of-bounds reads and use-after-free may lead to a denial-of-service (application crash) or other unspecified impact. • Non-maintainer upload by the ELTS team. • Fix CVE-2022-1851, CVE-2022-1898, CVE-2022-1968, CVE-2022-0943, CVE-2021-3903, CVE-2022-0417, CVE-2022-2124, CVE-2022-2126. Multiple security vulnerabilities have been discovered in vim, an enhanced vi editor. Buffer overflows, out-of-bounds reads and use-after-free may lead to a denial-of-service (application crash) or other unspecified impact.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- Non-maintainer upload by the ELTS team. - Fix CVE-2022-0572, CVE-2022-0261, CVE-2022-0351, CVE-2022-0413, CVE-2022-1720, CVE-2022-0443, CVE-2022-1616, CVE-2022-1619, CVE-2022-1621, CVE-2022-1154. Multiple security vulnerabilities have been discovered in vim, an enhanced vi editor. Buffer overflows, out-of-bounds reads and use-after-free may lead to a denial-of-service (application crash) or other unspecified impact. - Non-maintainer upload by the ELTS team. Fix the following CVE: CVE-2021-3872, CVE-2021-3927, CVE-2021-3928, CVE-2021-3973, CVE-2021-3974, CVE-2021-3984, CVE-2021-4019, CVE-2021-4069, CVE-2021-4192, CVE-2021-4193, CVE-2022-0213, CVE-2022-0319, CVE-2022-0359, CVE-2022-0361, CVE-2022-0368, CVE-2022-0408, CVE-2022-0554, CVE-2022-0685, CVE-2022-0714, CVE-2022-0729, CVE-2021-3796, CVE-2021-3778, CVE-2019-20807. Multiple security vulnerabilities have been discovered in vim, an enhanced vi editor. Buffer overflows, out-of-bounds reads and Null pointer derefrences may lead to a denial-of-service (application crash) or other unspecified impact.	

Last updated 2025-05-26 01:15:42 EDT

Unified v2.9.3 Security Updates, 2025-05-26

This document describes the 78 security updates available for Unified v2.9.3 base stations since the release, through 2025-05-26.

Date	Package	CVE(s)	Synopsys	Hardware Version
2023-12-17	ncurses-term	CVE-2023-29491	- Non-maintainer upload by the ELTS Team. - Mitigate CVE-2023-29491: Disallow loading of custom terminfo entries in setuid/setgid programs.	M400 S1600E M410 R100E S100 R100NA
2023-12-17	ncurses-bin	CVE-2023-29491	- Non-maintainer upload by the ELTS Team. - Mitigate CVE-2023-29491: Disallow loading of custom terminfo entries in setuid/setgid programs.	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
2023-12-17	libtinfo5	CVE-2023-29491	- Non-maintainer upload by the ELTS Team. - Mitigate CVE-2023-29491: Disallow loading of custom terminfo entries in setuid/setgid programs.	M400 S1600E M410 R100E S100 R100NA
2023-12-17	ncurses-base	CVE-2023-29491	- Non-maintainer upload by the ELTS Team. - Mitigate CVE-2023-29491: Disallow loading of custom terminfo entries in setuid/setgid programs.	M400 S1600E M410 R100E S100 R100NA
2023-12-20	libbluetooth3	CVE-2023-45866	- Non-maintainer upload by the Debian ELTS Team. - CVE-2023-45866: Fix an issue where Bluetooth Human Interface Devices (HID) hosts in BlueZ may have permitted an unauthenticated peripheral to initiate and establish encrypted connections and accept keyboard reports, potentially permitting injection of HID messages despite no user actually authorising such access.	M400 S1600E M410 R100E S100 R100NA
2024-01-26	libjasper1	CVE-2023-51257	- Non-maintainer upload by the ELTS team. - CVE-2023-51257 fix of invalid memory write	M400 S1600E M410 R100E S100 R100NA
2024-03-11	openssh-client	CVE-2023-51385 CVE-2021-41617	- Non-maintainer upload by the ELTS team. - Add debian/salsa-ci.yml using lts-team/pipeline for jessie - Fix test cert not yet valid by using cert dates after the end of jessie ELTS. Add debian/patches/test-fix-cer-not-yet-valid.patch - CVE-2023-51385: ssh(1): Ban most shell metacharacters from user and hostnames supplied via the command-line - CVE-2021-41617: Initialise correctly supplemental groups when executing an AuthorizedKeysCommand or AuthorizedPrincipalsCommand	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
2024-05-17	liblwres90	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash).	M400 S1600E M410 R100E S100 R100NA
2024-05-17	libdns-export100	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash).	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
2024-05-17	libbind9-90	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash).	M400 S1600E M410 R100E S100 R100NA
2024-05-17	libisccfg90	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash).	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
2024-05-17	libdns100	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash).	M400 S1600E M410 R100E S100 R100NA
2024-05-17	libisccc90	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash).	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
2024-05-17	libisccfg-export90	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash).	M400 S1600E M410 R100E S100 R100NA
2024-05-17	libirs-export91	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash).	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
2024-05-17	libisc95	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash).	M400 S1600E M410 R100E S100 R100NA
2024-05-17	libisc-export95	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash).	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
2024-05-17	bind9-host	CVE-2023-50387 CVE-2023-50387 CVE-2023-50868 CVE-2023-3341	• Non-maintainer upload by the ELTS Team. • CVE-2023-50387 and CVE-2023-50868 Specific DNS answers could cause a denial-of-service condition due to DNS validation taking a long time. (CVE-2023-50387) The same code change also addresses another problem: preparing NSEC3 closest encloser proofs could exhaust available CPU resources. (CVE-2023-50868) • Add debian/.gitlab-ci.yml using recipe for jessie • Add debian/tests/ from buster • Make d/tests/validation less flaky. • Non-maintainer upload by the ELTS Team. • CVE-2023-3341 A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash).	M400 S1600E M410 R100E S100 R100NA
2024-05-22	less	CVE-2022-48624	• No-change rebuild. • Non-maintainer upload by the ELTS team. • Fix CVE-2022-48624 and CVE-2024-32487: Several vulnerabilities were discovered in less, a file pager, which may result in the execution of arbitrary commands if a file with a specially crafted file name is processed.	M400 S1600E M410 R100E S100 R100NA
2024-06-17	nano	CVE-2024-5742	• Non-maintainer upload by the ELTS Team. • CVE-2024-5742: Emergency file symlink attack	M400 S1600E M410 R100E S100 R100NA
2024-06-30	locales	CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-	• Non-maintainer upload by the ELTS Team. • CVE-2024-33599: nscd: Stack-based buffer overflow in netgroup cache • CVE-2024-33600: nscd: Null pointer crashes after notfound response	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
		2024-33602 CVE-2024-2961	• CVE-2024-33601: nscd: Daemon may terminate on memory allocation failure • CVE-2024-33602: nscd: Possible memory corruption • Non-maintainer upload by the ELTS Team. • CVE-2024-2961: Out-of-bounds write in iconv ISO-2022-CN-EXT module	
2024-06-30	libc-bin	CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602 CVE-2024-2961	• Non-maintainer upload by the ELTS Team. • CVE-2024-33599: nscd: Stack-based buffer overflow in netgroup cache • CVE-2024-33600: nscd: Null pointer crashes after notfound response • CVE-2024-33601: nscd: Daemon may terminate on memory allocation failure • CVE-2024-33602: nscd: Possible memory corruption • Non-maintainer upload by the ELTS Team. • CVE-2024-2961: Out-of-bounds write in iconv ISO-2022-CN-EXT module	M400 S1600E M410 R100E S100 R100NA
2024-06-30	libc6	CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602 CVE-2024-2961	• Non-maintainer upload by the ELTS Team. • CVE-2024-33599: nscd: Stack-based buffer overflow in netgroup cache • CVE-2024-33600: nscd: Null pointer crashes after notfound response • CVE-2024-33601: nscd: Daemon may terminate on memory allocation failure • CVE-2024-33602: nscd: Possible memory corruption • Non-maintainer upload by the ELTS Team.	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
			- CVE-2024-2961: Out-of-bounds write in iconv ISO-2022-CN-EXT module	
2024-06-30	multiarch-support	CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602 CVE-2024-2961	- Non-maintainer upload by the ELTS Team. - CVE-2024-33599: nscd: Stack-based buffer overflow in netgroup cache - CVE-2024-33600: nscd: Null pointer crashes after notfound response - CVE-2024-33601: nscd: Daemon may terminate on memory allocation failure - CVE-2024-33602: nscd: Possible memory corruption - Non-maintainer upload by the ELTS Team. - CVE-2024-2961: Out-of-bounds write in iconv ISO-2022-CN-EXT module	M400 S1600E M410 R100E S100 R100NA
2024-08-03	libcurl3	CVE-2024-7264	- Non-maintainer upload by the ELTS team. - Fix CVE-2024-7264: A denial-of-service vulnerability was found in cURL, an easy-to-use client-side URL transfer library. libcurl's ASN1 parser code has the GTime2str() function, used for parsing an ASN.1 Generalized Time field. If given an syntactically incorrect field, the parser might end up crashing but this flaw can also lead to heap contents getting returned to the application when CURLINFO_CERTINFO is used.	M400 S1600E M410 R100E S100 R100NA
2024-08-03	curl	CVE-2024-7264	- Non-maintainer upload by the ELTS team. - Fix CVE-2024-7264: A denial-of-service vulnerability was found in cURL, an easy-to-use client-side URL transfer library. libcurl's ASN1 parser code has the GTime2str() function, used for parsing an ASN.1 Generalized Time field. If given an syntactically incorrect field, the parser might end up crashing but this flaw can also lead to heap contents getting returned to the application when CURLINFO_CERTINFO is used.	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
2024-08-12	libgdk-pixbuf2.0-0	CVE-2022-48622	• Non-maintainer upload by the ELTS Team. • CVE-2022-48622: ANI file loader memory corruption	M400 S1600E M410 R100E S100 R100NA
2024-08-12	libgdk-pixbuf2.0-common	CVE-2022-48622	• Non-maintainer upload by the ELTS Team. • CVE-2022-48622: ANI file loader memory corruption	M400 S1600E M410 R100E S100 R100NA
2024-08-14	libsmartcols1	CVE-2024-28085 CVE-2021-37600	• Non-maintainer upload by the Debian ELTS team. • Fix CVE-2024-28085: Escape sequence injection in wall(1). • d/rules: Build with --disable-use-tty-group to avoid installing wall(1) setgid tty. • Re-upload based 2.25.2-6, not 2.26.2-6. • Non-maintainer upload by the Debian ELTS team. ○ CVE-2021-37600: sys-utils/ipcutils: be careful when call calloc() for uint64 nmembs • Remove existing debian/gbp.conf. • Add debian/.gitlab-ci.yml; allow piuparts and lintian failures.	M400 S1600E M410 R100E S100 R100NA
2024-08-14	libuuid1	CVE-2024-28085 CVE-2021-37600	• Non-maintainer upload by the Debian ELTS team. • Fix CVE-2024-28085: Escape sequence injection in wall(1). • d/rules: Build with --disable-use-tty-group to avoid installing wall(1) setgid tty. • Re-upload based 2.25.2-6, not 2.26.2-6. • Non-maintainer upload by the Debian ELTS team.	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ CVE-2021-37600: sys-utils/ipcutils: be careful when call calloc() for uint64 nmembs • Remove existing debian/gbp.conf. • Add debian/.gitlab-ci.yml; allow piuparts and lintian failures.	
2024-08-14	hostapd	CVE-2024-5290 CVE-2023-52160	• Non-maintainer upload by the ELTS Team. • CVE-2024-5290: Only load libraries from trusted path • Non-maintainer upload by the ELTS Team. • Add salsa CI • Fix CVE-2023-52160: The implementation of PEAP in wpa_supplicant allows authentication bypass. For a successful attack, wpa_supplicant must be configured to not verify the network's TLS certificate during Phase 1 authentication, and an eap_peap_decrypt vulnerability can then be abused to skip Phase 2 authentication. This allows an adversary to impersonate Enterprise Wi-Fi networks.	M400 S1600E M410 R100E S100 R100NA
2024-08-14	libblkid1	CVE-2024-28085 CVE-2021-37600	• Non-maintainer upload by the Debian ELTS team. • Fix CVE-2024-28085: Escape sequence injection in wall(1). • d/rules: Build with --disable-use-tty-group to avoid installing wall(1) setgid tty. • Re-upload based 2.25.2-6, not 2.26.2-6. • Non-maintainer upload by the Debian ELTS team. ○ CVE-2021-37600: sys-utils/ipcutils: be careful when call calloc() for uint64 nmembs • Remove existing debian/gbp.conf.	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Add debian/.gitlab-ci.yml; allow piuparts and lintian failures.	
2024-08-14	mount	CVE-2024-28085 CVE-2021-37600	• Non-maintainer upload by the Debian ELTS team. • Fix CVE-2024-28085: Escape sequence injection in wall(1). • d/rules: Build with --disable-use-tty-group to avoid installing wall(1) setgid tty. • Re-upload based 2.25.2-6, not 2.26.2-6. • Non-maintainer upload by the Debian ELTS team. ○ CVE-2021-37600: sys-utils/ipcutils: be careful when call calloc() for uint64 nmembs • Remove existing debian/gbp.conf. • Add debian/.gitlab-ci.yml; allow piuparts and lintian failures.	M400 S1600E M410 R100E S100 R100NA
2024-08-14	libmount1	CVE-2024-28085 CVE-2021-37600	• Non-maintainer upload by the Debian ELTS team. • Fix CVE-2024-28085: Escape sequence injection in wall(1). • d/rules: Build with --disable-use-tty-group to avoid installing wall(1) setgid tty. • Re-upload based 2.25.2-6, not 2.26.2-6. • Non-maintainer upload by the Debian ELTS team. ○ CVE-2021-37600: sys-utils/ipcutils: be careful when call calloc() for uint64 nmembs • Remove existing debian/gbp.conf. • Add debian/.gitlab-ci.yml; allow piuparts and lintian failures.	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
2024-08-14	util-linux	CVE-2024-28085 CVE-2021-37600	• Non-maintainer upload by the Debian ELTS team. • Fix CVE-2024-28085: Escape sequence injection in wall(1). • d/rules: Build with --disable-use-tty-group to avoid installing wall(1) setgid tty. • Re-upload based 2.25.2-6, not 2.26.2-6. • Non-maintainer upload by the Debian ELTS team. ○ CVE-2021-37600: sys-utils/ipcutils: be careful when call calloc() for uint64 nmembs • Remove existing debian/gbp.conf. • Add debian/.gitlab-ci.yml; allow piuparts and lintian failures.	M400 S1600E M410 R100E S100 R100NA
2024-08-14	bsdutils	CVE-2024-28085 CVE-2021-37600 CVE-2014-9114 CVE-2014-9114 CVE-2007-5191	• Non-maintainer upload by the Debian ELTS team. • Fix CVE-2024-28085: Escape sequence injection in wall(1). • d/rules: Build with --disable-use-tty-group to avoid installing wall(1) setgid tty. • Re-upload based 2.25.2-6, not 2.26.2-6. • Non-maintainer upload by the Debian ELTS team. ○ CVE-2021-37600: sys-utils/ipcutils: be careful when call calloc() for uint64 nmembs • Remove existing debian/gbp.conf. • Add debian/.gitlab-ci.yml; allow piuparts and lintian failures. • Add patch to fix unshare -r regression. ○ Cherry-picked upstream commit 0bf159413bdb9e32486 "unshare: Fix --	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
			map-root-user to work on new kernels" Thanks to Kirill Smelkov • Revert "Trigger update of initramfs on upgrades" • Revert "Add Breaks: live-tools (<<4.0~alpha17-1)" ○ No longer needed since dropping the update-initramfs call. • Fix typo in symlink_to_dir and bump prior-version ○ in other words, fix 2.25.2-4.1 upload. • Add Breaks: grml-debootstrap (<< 0.68) ○ previous versions does not work properly with new util-linux which always identifies atleast one label for every partition (PARTUUID) so lets prevent partial upgrades. • Non-maintainer upload. • Add Breaks: live-tools (<<4.0~alpha17-1) • Non-maintainer upload. • Fix unhandled symlink_to_dir conversion for /usr/share/doc/libblkid-dev • Update POT and PO files and clean up .gmo files • Update German translation, thanks to Mario Blättermann • Update Spanish translation, thanks to Antonio Ceballos Roa • Update French translation • Update Ukrainian translation, thanks to Yuri Chornoivan • Update Brazilian Portuguese translation, thanks to Rafael Ferreira	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Update Chinese (simplified) translation, thanks to Wylmer Wang • Update Danish translation, thanks to Joe Hansen • Update Finnish translation, thanks to Lauri Nurmi • Update Japanese translation, thanks to Takeshi Hamasaki • Update Russian translation, thanks to Pavel Maryanov • Trivial unfuzzy • Add debian/patches/libblkid-care-about-unsafe-chars-in-cache.patch ○ from upstream git master commit 89e90ae7 "libblkid: care about unsafe chars in cache" ○ This fixes CVE-2014-9114: blkid command injection see https://security-tracker.debian.org/tracker/CVE-2014-9114 Thanks to Salvatore Bonaccorso • libuuid1: add passwd dependency for user migration • Ship fstrim timer/service units as examples only ○ this works around #757891 and #767429 / #760168 • Only ship fstrim service and timer on linux • Imported Upstream version 2.25.2 • Rebase patch queue on top of v2.25.2 ○ This drops the following patches now included upstream: Report-correct-disk-size-on-GNU-kFreeBSD.-Thanks-Tuc.patch remaining-kFreeBSD-hackery-for-building.patch 2.20.1-1.2.patch kFreeBSD-add-hacks-in-ipcrm-to-avoid-FTBFS.patch libmount-only-invoke-loopcxt-on-linux.patch libmount-only-include-context-on-	

Date	Package	CVE(s)	Synopsys	Hardware Version
			linux.patch build-sys-build-libmount-everywhere.patch build-sys-use-lutil-for-BSD-only.patch libmount-fix-mnt_is_readonly-ifdef.patch flock-zero-timeout-is-valid.patch build-sys-check-for-libtoolize-rather-than-libtool.patch script-may-be-hangs.patch ● Ship fstrim service and timer ● Add debian/patches/build-sys-check-for-libtoolize-rather-than-libtool.patch ○ Cherry-picked from upstream commit e71b0aadaa20b21e9 "build-sys: check for libtoolize rather than libtool" Thanks to Helmut Grohne for fixing this upstream (and more). ● Add debian/patches/script-may-be-hangs.patch ○ Cherry-picked from upstream commit 032228c9af6fbda5177c "script: may be hangs" ● Use usermod instead of chsh in postinst user migration ● Use a single usermod call in postinst user migration ● Silence the attempt to stop uuidd before migration ● Pass -std=gnu99 to CC when cross-building. ● Add debian/patches/libmount-fix-mnt_is_readonly-ifdef.patch ○ Cherry-picked from upstream commit 473c5fb86c43eed "libmount: fix mnt_is_readonly() #ifdef" ○ Fixes Hurd build failure. Thanks to Pino Toscano for fixing this upstream! ● hwclock-set: use both systz and hctosys. Thanks to Ben Hutchings for debugging this. ● Add debian/patches/flock-zero-timeout-is-valid.patch	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ Cherry-picked from upstream commit c4604c38b503c8c46e "flock: zero timeout is valid" • Trigger update of initramfs on upgrades • hwclock-set: Don’t use 'touch' to create stamp file, as it may not be included in an initramfs (Really • Put uuid-runtime in Section utils. Thanks to Ben Finney for the suggestion • Cherry-pick upstream commit 8026fa9bc752 "build-sys: use -lutil for BSD only" debian/patches/build-sys-use-lutil-for-BSD-only.patch • Upload to unstable. • Make libmount-dev depend on libblkid-dev (LP: #1096581) • Drop uuid-dev dependency in libmount-dev package • Drop explicit disabling of pivot_root on non-linux • Attempt to stop uuidd before usermod in postinst (LP: #1374648) • Change build-dep to new unified libsystemd-dev • hwclock-set: Use stamp file in /run/udev to ensure we set the clock only once if installed in the initramfs • Rename libuuid user to uuidd in libuuidd1 postinst as well • Imported Upstream version 2.25.1 • Drop duplicated BSD-3-clause license text from debian/copyright • Restart uuidd /after/ upgrade. Thanks to Michael Biebl for the suggestion. • Cherry-pick fdisk/bsd test fix from upstream. Thanks to Aurélien Jarno for solving and submitting this upstream	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Imported Upstream version 2.25.1~rc1 • Rebase debian patch set on top of 2.25.1~rc1 ○ Drop patches for things fixed in new upstream release: debian/patches/cfdisk-reenable-cursor-when-quitting.patch debian/patches/fdisk-fix-l-device.patch debian/patches/tests-allow-non-inotify-tailf-to-keep-up.patch debian/patches/tests-fix-fdisk-bsd-for-the-two-possible-sectors-off.patch ○ Refresh remaining patches. • Mark libmount context symbols linux-any • Add patches to make libmount build on kfreebsd • Mark libmount1 as to be built everywhere • Install fsck on every architecture • Add NEWS entry about reinstating fsck on kFreeBSD. Disclaimer: I, Andreas Henriksson, will **not** maintain the patches. • Only install linux32/64 manpages on linux-any • Fix uuid-runtime.postinst to skip rmdir when not needed • fdisk-udeb: use dh-exec to skip sfdisk install on sparc • Mangle installed files on sparc (sfdisk) • Fix sparc install mangling • Use --disable-mountpoint instead of rm • Use dh-exec (>= 0.13) • Install mips,ppc,s390 setarch symlinks and manpages The "Jonno was here" release.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Drop changelog file from the ancient mount source package. • util-linux: Drop all (obsolete) Replaces/Conflicts • Add Replaces/Breaks bash-completion (<< 1:2.1-3). • Multiple cleanups in debian/control. • Minor cleanup of debian/rules. • Use filter, not findstring, for arch matching • Simplify linux-only install file handling • Use debian/*-udeb.install files for udeb packages. • Fix util-linux lintian override. • Minor uuid-runtime.postinst cleanup • Add d/p/cfdisk-reenable-cursor-when-quitting.patch The "big maintainer-script cleanup" release • Drop debian/uuid-runtime.prerm (and related lintian override) ○ dh_installinit will automatically start and stop services as needed. • Drop debian/libuuid1.postinst (user/group addition) • uuid-runtime: improved user/group handling ○ pre-depend on new libuuid1 to make sure no old user handling is present ○ add code to rename existing libuuid user/group to uuidd and set nologin shell and new home directory. ○ switch to adduser instead of opencoding it since uuid-runtime is Priority: optional (as opposed to libuuid1 which is required) and adduser --system should just do the right thing.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ change user/group addition to add uuidd instead of libuuid. ○ stop making uuidd setuid, not needed and we don’t want anyone to be able to kill the daemon (via uuidd -k) for example. ● Drop d/p/Use-libuuid-user-group-in-sysvinit-script-systemd-un.patch ● util-linux: drop obsolete hwclock handling from maint-scripts ● util-linux: drop obsolete update-mime calls ● util-linux: drop obsolete 2.17 upgrade warning ● util-linux: drop obsolete /etc/default/rcS → /etc/adjtime migration ● Reindent/cleanup all maintainer scripts ● Drop outdated debian/README.Debian.hwclock ● Drop unused debian/rejected-upstream ● Drop outdated debian/uuid-dev.README.Debian ● Drop diffutils build-dependency ● Drop debian/*.dirs ● Attempt to avoid dumb term problem in "more: regexp" test ● Minor improvements to verbose-tests.patch ● Drop renice bash completion for now ● Include dpkg-dev’s pkg-info.mk to get package version ● Stop creating unused /etc/fstab.d directory ● Use proper getty [hurd-any] for Conflicts/Replaces	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Add patches cherry-picked from upstream git master ○ debian/patches/tests-allow-non-inotify-tailf-to-keep-up.patch fixes failing testcase on hurd/kfreebsd. ○ debian/patches/fdisk-fix-l-device.patch fixes regression in fdisk listing partition. • Don’t ship dmesg bash-completions for now • Add verbose-tests.patch to get more info from tests • Make testsuite non-fatal for now • Add runuser pam configuration from Fedora • Install bash-completion for selected utilities • Prevent dh_installman from messing up rename.ul manpage • Drop misplaced Multi-Arch property on libblkid1-udeb • Set system time directly from hw clock in udev rule • Don’t require nfs-common on NFS-rooted system • Fine-tune hwclock.sh init script LSB dependencies • Keep mandatory Required-Stop LSB header in hwclock.sh init script • Revert "Disable tests for now" • Fix binary-arch only builds • Imported Upstream version 2.25 • Rebase patch queue on top of new upstream release + Drop debian/patches for unused and removed mount-deprecated ○ tries-to-umount-proc-when-told-to-umount-some-dir-pr.patch	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ mount-segfault-when-creating-mtab-and-cannot-determi.patch + Update cfdisk.8 patch to modify new manpage file. + Remaining changes are all trivial refreshes. • Update debian/README.source instructions • Fix PPC fdisk/ddisk rename in debian/rules • Stop installing cytune which is no longer available • Use new consolidated systemd configure option • Add util-linux.NEWS entry • Explicitly configure without python for now • Only install i386 and x86_64 binaries on selected architectures • Add new libsmartcols packages • Update libblkid and libmount symbols/shlibs • Drop unused and uninstallable libmount1-udeb • Update debian/copyright for upstream v2.25 • util-linux: Install new terminal-colors.d(5) manpage • Explicitly disable unused utilities • Use correct configure options on non-linux • Add debian/patches/kFreeBSD-add-hacks-in-ipcrm-to-avoid-FTBFS.patch ○ fixes build failure in ipcrm on kFreeBSD • Skip installing a whole bunch of utils on non-linux • Add WARNING about missing fsck on non-linux to util-linux.NEWS	

Date	Package	CVE(s)	Synopsys	Hardware Version
			● new branch, with separated patches. ● New upstream release ● Rebase patches/v2.20.1 branch (commit ad744ecf) on upstream v2.24.2 tag ○ drop patches for issues that has been fixed upstream: [8f1c9b31] "Fix cve-2013-0157: mount discloses information about …" [f08936ba] "sfdisk: fix calculation due to type mismatch (ix86)" [3f051232] "Fix typo in misc-utils/blkid.c" [b9b0ed84] "drop my_dev_t.h, based on 88d52b16ce4df…" (Squashed into man-page-tweaks-cleanup-my_dev_t.h-ancient-stuff.patch) [9ecca8da] "sparc-utils 'sparc64' binary sets ADDR_LIMIT_32BIT. …" [b153d64e] "Fix typo in unshare manpage." [01cfac31] "agetty: don't use log_err() for non-fatal errors" ○ drop translation updates conflicting with upstream translation updates: [83bc98c2] "Translation updates, various bugs." ○ drop patch for feature deprecated upstream: [23c9f34b] "hash passphrases - debian compatibility" (losetup encryption support dropped, use cryptsetup.) ● debian/source/format: switch to 3.0 (quilt) ● gbp-pq export patches in quilt format from rebased branch ● debian/watch: fix it - use http and xz extension ● debian/control: use source:Upstream-Version instead of reinventing it ● Switch to dh7 rules and use dh-autoreconf ● bsdutils: don't try to install removed files ● Bump debhelper compat to 9	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Update libblkid1 and libmount1 with added symbols • Documentation files has been moved/renamed ○ also ship all release notes • util-linux-locales: use wildcard to catch all locales • Upstream no longer ships ddate • Drop obsolete --enable-rdev configure switch • Run wrap-and-sort • Add systemd [linux-any] build dependency ○ gets rid of an ugly configure warning • Bump Standards-Version to 3.9.5 • Incorporate NMU changelogs for 2.20.1-5.[678] ○ Their actual changes are all obsoleted by upstream changes. • Install upstream fstab example in mount docs dir • Install debian fstab example in mount again under new name • Add debian/util-linux.NEWS documenting major changes • Install manpages in util-linux package • Use dh_installinit to install hwclock init.d and default files • Install getopt-parse bash and tcsh examples in util-linux docs dir • Let dh_installmime install util-linux mime config • Let dh_installdirs create /etc/fstab.d/	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Split up old debian/rules hacks further • lintian said mount needed ${misc:Depends} dependency • Add mount/losetup encryption NEWS and recommend cryptsetup • debian/watch: use https url • debian/copyright: update and make machine readable (DEP-5) • Add debian/gbp.conf • Add myself to uploaders, with Adam Conrads blessing. • Point Vcs-* fields to new collab-maint repository • debian/gbp.conf: gbp-pq --no-patch-numbers • Drop Homepage field • Bump shlibs to latest API according to symbols • Fix hwclock.sh to add a final newline in /etc/adjtime • Stop installing extra license files • debian/copyright: Add missing License paragraphs • debian/gbp.conf: Enable pristine-tar • Imported Upstream version 2.24.2 • Add debian/README.source • Improve package descriptions • Improve bsdutils package description • Use simple (ascii) punctuation marks in debian/changelog	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ replaces fancy utf-8 characters in 2.20.1-1.1 and 2.17.2-3.1 • Use ${misc:Pre-Depends} instead of hardcoding multiarch-support • Fix dh_makeshlibs to add udebs in generated shlibs • Multi-arch -dev packages • Add missing Multi-Arch line to libmount1 package • Put util-linux-locales in section localization • Fix check for systemd in hwclock-set udev script • Fix mismerge in remaining-kFreeBSD-hackery-for-building.patch • Remove /usr/doc/libblkid-dev symlink in postinst/prerm • Add patch to use "libuuid" user/group instead of "uuidd" • Install uuidd sysvinit script and systemd units • Explicitly configure with socket activation enabled • Ship new utilities chcpu, blkdiscard, wdctl, resizepart, lslocks, nsenter, prlimit, utmpdump • Build-depend on libpam0g-dev and ship runuser utility • Ship mkfs.cramfs and fsck.cramfs manpages • Drop obsolete configure switch enable-libmount-mount • Override localstatedir to /run instead of /var • Ship runuser manpage • Add ppc64el to archs where fdisk is renamed ddisk	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Attempt to reinstate cross-building support • Disable tests for now ○ Requires network access and prints scary warnings • Fix Multiarch-support-in-util-linux-build.patch ○ Make sure @libexecdir@ gets expanded in pkg-config files • Non-maintainer upload. • misc-utils/wipefs.c: In --all mode, wipe several times until no further signatures are found. This is required for file systems like VFAT which can be detected in multiple different ways. This is fixed properly in 2.21 (see LP #1012081), but does not backport well, so use this local hack for now. (LP: #1046665, • Non-maintainer upload. • Add arm64/aarch64 support • Non-maintainer upload. • Fix m4 looping in configure.ac's _UTIL_CHECK_SYSCALL. m4_shiftn(2, sequence of two elements) infloops. • mount should not strip MS_REC for --make-r* options. • Non-maintainer upload by the Security Team. • Fix cve-2013-0157: mount discloses information about the existence of folders • Non-maintainer upload. • Rebuild against new eglibc; no source changes. libblkid.a uses the symbol __secure_getenv which is no longer present (it provides secure_getenv). • Non-maintainer upload.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Ship the /var/lib/libuuid/ directory in the package instead of creating it in postinst. • Non-maintainer upload. • Drop the /etc/default/rcS update from postinst. • French, David Prévot. • Vietnamese, Trần Ngọc Quân. • Dutch, Benno Schulenberg. • Polish, Michał Kułach. • Non-maintainer upload. • agetty: don’t use log_err() for non-fatal errors • agetty: Eliminate another log_err() call. • Fix watch file • sfdisk: fix calculation due to type mismatch (ix86) • Make sure we have non-null mount options. • tries to umount /proc when told to umount /some/dir/proc without an /etc/mtab entry. • Deliver {c,}fdisk-udeb on hurd. • Improve handling of the hardware clock ○ Remove redundant hwclockfirst.sh and hwclock.sh. The reason for this redundant script existing (/etc/localtime not being present until after /usr was mounted AFAICT) no longer exists. The hwclock script has been adjusted to run before checkroot. ○ Migrate existing UTC= setting in /etc/default/rcS to UTC/LOCAL in /etc/adjtime. This removes needless duplication of the setting, and prevents the behaviour of hwclock being	

Date	Package	CVE(s)	Synopsys	Hardware Version
			overridden, and its configuration overwritten every shutdown. ○ The hwclock init scripts now use /etc/adjtime instead of the --utc and --localtime options (based on the UTC setting). ○ Add /etc/default/hwclock and hwclock(5) which permit configuration without editing the initscript, and also document all the undocumented variables used by the scripts. ○ The udev hwclock-set script runs hwclock --tzset unconditionally in all cases (it's a no-op for UTC). ○ The user running "hwclock --systohc (--utc|--localtime)" is now handled correctly. The clock state is recorded in /etc/adjtime and correctly handled on system restart. This means the UTC setting in /etc/default/rcS doesn't create problems by requiring two separate changes (changing the UTC setting and running hwclock) to do the same thing. ○ Comment out the now-obsolete UTC= setting in /etc/default/rcS, with a reference to /etc/adjtime and hwclock(8). ○ systemd uses /etc/adjtime as for hwclock to store the hardware clock UTC/LOCAL configuration. This change means there's a single place to store the hardware clock configuration for all init systems. • Polish Debconf Translation. • fix lintian error • Drop broken Pre-Depends: multiarch-support on udeb. • Support /etc/default/hwclock. • fix lintian error	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Better english in mount.8. • Multiarch support in util-linux build. • Drop ancient and technically incorrect workaround for hwclock ordering in postinst. • Re-enable ddate, disabled by default upstream in 2.20. • Ack 2.20.1-1.2 • Re-enable ddate. • reenable line. • Deliver the correct upstream changelog. • Fix typo in misc-utils/blkid.c. • fix FTBFS on !linux-any. • Preserve the ACPI wakeup time when updating the hardware clock. • Fix typo in unshare manpage. • Enable hardened build flags. • Non-maintainer upload. • Fixing FTBFS on !linux • Only enable partx where it is supported • Handle vc flags missing on FreeBSD • Fix tty creation on kFreeBSD taking patch from 2.19 • Non-maintainer upload. • Fix FTBFS by running autoreconf -vfi before calling ./configure, which looks better than patching	

Date	Package	CVE(s)	Synopsys	Hardware Version
			Makefile.in’s manually. Thanks to Thorsten Glaser for reporting, and to Simon Ruderich for suggesting a patch • Add autoconf, automake, autopoint, and libtool to Build-Depends accordingly. • Set severity to "high" for the RC bug fix. • New upstream • Various merge fixes [with edits - lamont] ○ drop old unused patches ○ cleanup debian/rules ○ updated symbols files for lib{blkid,mount,uuid}1 • merge in 2.19.1-{3..5} • deliver /etc/fstab.d • add korean debconf pofile. • Add build-arch and build-indep targets. • Conflict/Replace fstrim to provide smooth upgrades • Don’t run hwclock-set when running under systemd • Switch to using linux-any in place of lists • Add missing patch from #631468 to fix agetty linkage on k*bsd • Apply two patches from Michael Biebl <biebl@debian.org>: ○ disable libmount on !linux, fixing kfreebsd FTBFS ○ remove empty /usr/share/locale/ from util-linux	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Apply patch from Roger Leigh <rleigh@debian.org> to make hwclock.sh correctly support /run/udev in addition to /dev/.udev • Build with arch:all to resurrect util-linux-locales • Add myself to Uploaders, following a short conversation with LaMont. • deliver findmnt in mount, rather than util-linux • Dutch transations. • Japanese translation. • Finnish debconf templates. • Update with current translations • Enable libmount; new packages libmount1, libmount-udeb and libmount-dev added; bump standards-version • update Indonesian translations. • debconf po file for Catalan. • Add Homepage: to control. • New upstream • NMU • Bump to Standards-Version 3.9.1. • Drop XS- prefixes on Vcs-Git and Vcs-Browser fields. • Patch from Konstantinos Margaritis to add preliminary armhf support. • Add watch file. • Ack NMU from Christian Perrier <bubulle@debian.org>	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ Fix encoding for Danish and Slovak debconf translations • Brazilian Portuguese debconf templates translation. • fix mangled characters in debconf translations • dh_installdebconf is needed in binary-arch, not so much in -indep. Based on report from Adam D. Barratt <adam@adam-barratt.org.uk>. • nb translations. • Portuguese debconf translations. • Italian translations. • russian debconf translations. • Swedish debconf translations. • Danish translations. • French debconf translations. • German debconf translations. • Spanish debconf translations. • hwclock: [m68k] unbreak FTBFS with recent (>= 2.4.18?) kernels. • Slovak transtions. • Czech debconf translations. • Merge in all those NMUs that were never pushed to me in bugs. • mount: don’t canonicalize "spec" with --no-canonicalize option. • fdisk: fix freespace boundaries calculation on SGI disklabel.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Deliver agetty as both agetty and getty, preferring agetty. • Declare source format (1.0) • use debconf (iff installed) to warn about noauto fileysstems with non-zero pass numbers. • update lintian-overrides, actually install them in the deb • Non-maintainer upload. • Report correct disk size on GNU/kFreeBSD. Thanks Tuco. • Non-maintainer upload. • Revert the switch from slang2 to ncurses5. There is no udeb for ncurses, so that change broke cfdisk-udeb • Non-maintainer upload. • Apply trivial patch by Adam D. Barratt (thanks!): Only attempt to link locale-specific files in to the cfdisk-udeb hierarchy if cfdisk-udeb is actually being built. • Set urgency to "high" since some packages are waiting for util-linux. • Switch from slang2 to ncurses5. • Merge remote branch 'origin/stable/v2.17' into stable/v2.17 • Restore dropped dep on initscripts. • Add preliminary powerpcspe support. • should build Depend: dpkg or install-info. • pretty up the removal of /usr/share/info/dir • Fix fallocate configure check.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• libblkid: reset BLKID_TINY_DEV flag in blkid_probe_set_device • mount: posix option of vfat is obsolete • mount: update documentation about barrier mount options • sfdisk: confused about disk size • mount: fix typo in mount.8 • fdisk: sleep-after-sync and fsync usage • lscpu: add {32,64}-bit CPU modes detection • tests: refresh lscpu tests • docs: update AUTHORS file • docs: update v2.17 ReleaseNotes • build-sys: release++ (v2.17) • fdisk: don’t include scsi.h • libblkid: restrict RAID/FS proving for small devices (1.4MiB) • libblkid: read() optimization for small devices • tests: fix RAIDs tests • libblkid: call read() per FAT root dir entry • libblkid: set minimal size for jfs, reiser, swap and zfs • libblkid: read whole SB buffer (69kB) on large disks • libblkid: don’t call read() per FAT dir-entry on large disks • libblkid: add minimal sizes for OCFS and GFS	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- tests: update FS test images - libblkid: rewrite blkid_probe_get_buffer() - blkid: probe for PT, don't probe for FS on small whole-disks - libblkid: add sanity checks for FAT to DOS PT parser - libblkid: don't probe for GPT and Unixware PT on floppies - login: don't link PAMed version with libcrypt - libblkid: more robust minix probing - blkid: add newline when only one value is printed - login: check that after tty reopen we still work with a terminal - fdisk: use optimal_io_size - fdisk: use "optimal I/O size" in warnings - wipefs: ignore devices with partition table - libblkid: don't return error on empty files - fdisk: don't check alignment_offset against geometry - fdisk: fix check_alignment() - fdisk: cleanup alignment, default to 1MiB offset - fdisk: fix default first sector - fdisk: cleanup warnings - tests: add fdisk alignment tests - tests: fix and update old fdisk tests	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• mount: warn users that mtab is read-only • cal: fix first day of the week calculation on BE systems • build-sys: remove duplicate #includes • blkid: fix #ifdef HAVE_TERMIO[S]_H • build-sys: add missing tests for libuuid and libblkid • mount: advise users to use "modprobe", not "insmod" • include: add min/max macros • fdisk: use more elegant way to count and check alignment • tests: update fdisk tests • fdisk: cleanup help, add -h option • fdisk: fallback for topology values • fdisk: fix ALIGN_UP • fdisk: add -c option (switch off DOS mode) • fdisk: use 1MiB offset and grain always when possible • tests: update fdisk tests • fdisk: don’t use 1MiB grain on small devices • blkid: report open() errors in low-level probing • tests: update fdisk tests (add whitespaces) • docs: update AUTHORS file • docs: add v2.17.1 ReleaseNotes • build-sys: release++ (v2.17.1-rc1)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• swapon: fix swapsize calculation • fdisk: swap VTOC values for warning messages • docs: update AUTHORS file • docs: update v2.17.1 ReleaseNotes • build-sys: release++ (v2.17.1) • docs: fix small typo in v2.17.1-ReleaseNotes • libblkid: support alignment_offset=-1 • libblkid: more robust minix probing • libblkid: fix display of device size • swapon: remove " (deleted)" from filenames from /proc/swaps • libblkid: remove "0x" prefix from DRBD UUID • wipefs: cleanup usage() and man page • mount: more explicitly explain fstab usage in mount.8 • lib: add #ifndef around min() max() macros • fdisk: fix -b <sectorsize> • docs: update AUTHORS file • docs: add v2.17.2 ReleaseNotes • build-sys: release++ (v2.17.2) • po: merge changes • namei: fix man page formatting • cfdisk: set '[Quit]' as default menu item on first run instead of '[Bootable]'.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• cfdisk: set '[New]' as default item on menu for non allocated space instead of '[Help]'. • libblkid: fix ZSF detection • libblkid: DRBD support for blkid • libblkid: fix segfault in drdb • sfdisk: make sure writes make it to disk in write_partitions() • libblkid: disable read-ahead when probing device files • ionice: fix typo • pg: command enters infinite loop • mount: properly ignore comments in /etc/filesystems • new upstream • lintian cleanup • updated symbols file for libblkid1 • drop use of install-info in postinst, uses triggers now • adjust mount.8 manpage to avoid man error • lscpu: fix cpuid opcode detection • login: use fd instead of pathname for update tty’s owner and permissions • libblkid: fix infinite loop when probe chain bails out early • po: update id.po (from translationproject.org) (Arif E. Nugroho) • po: update ja.po (from translationproject.org) (Makoto Kato)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- po: update cs.po (from translationproject.org) (Petr Pisar) - po: update eu.po (from translationproject.org) (Mikel Olasagasti Uranga) - po: update eu.po (from translationproject.org) (Mikel Olasagasti) - po: update zh_CN.po (from translationproject.org) (Ray Wang) - po: update pl.po (from translationproject.org) (Jakub Bogusz) - po: update vi.po (from translationproject.org) (Clytie Siddall) - po: update fi.po (from translationproject.org) (Lauri Nurmi) - flock: fix hang when parent ignores SIGCHLD - docs: update TODO list - docs: update AUTHORS file - docs: update v2.17 ReleaseNotes - build-sys: release++ (v2.17-rc2) - lib: bug (typo) in function MD5Final() - docs: add ngettext() into TODO file - docs: update v2.17 ReleaseNotes - build-sys: release++ (v2.17-rc3) - docs: add LGPLv2+ to list of licenses - libblkid: fix Adaptec RAID detection - libblkid: fix highpoint37x detection	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• libblkid: rename highpoint RAIDs to hpt{37,45}x_raid_member • tests: add adaptec RAID test • tests: add hpt37x RAID test • tests: add hpt45x RAID test • tests: add isw RAID test • tests: add jmicron RAID test • tests: add lsi RAID test • tests: add nvidia RAID test • tests: add promise RAID test • tests: add silicon RAID test • mount: disable --no-canonicalize for non-root users • umount: add --no-canonicalize • po: merge changes • po: fix msgid bugs • po: merge changes • po: update pl.po (from translationproject.org) (Jakub Bogusz) • po: update cs.po (from translationproject.org) (Petr Pisar) • po: update eu.po (from translationproject.org) (Mikel Olasagasti Uranga) • New upstream version	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• hwclockfirst.sh: initscript LSB header in conflict with update-rc.d options. • hwclock*.sh: one more round of header tweaks. • Acknowledge Aurelien Jarno NMU • Non-maintainer upload. • Upload to unstable. • Don’t ship *.la files. • Add avr32 to debian/control • Remove the outdated debian/shlibs.local file. • Remove the auto-update of symbols files from debian/rules. • Remove symbols from the debian/libuuid1.symbols files which were never part of the public ABI, like uuid_pack/uuid_unpack and were falsely copied over from e2fsprogs. • Strip the Debian revision in the symbols files. • Create a shlibs file for libblkid1 and libuuid1 and bump it to >= 2.16 to ensure correct udeb shlibs dependencies. • Remove *.la files and empty /usr/include and /usr/lib/pkgconfig directories from the util-linux package. • Only check for ENOMEDIUM when ENOMEDIUM is defined. Fixes build on GNU/kFreeBSD. • hwclock: fix mismatched popen/fclose. • ionice: Allow setting the none class • build-sys: fix "make -C" bug • build-sys: fix blkid.h include for old e2fsprogs	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• blkid: make libuuid optional • build-sys: rename /libs to /shlibs • build-sys: complete /libs to /shlibs rename • blkid: fix "hangs forever with partition type mdraid" • blkid: blkid_do_safeprobe() has to be tolerant to RAIDs • blkid: cleanup debug messages and return codes in blkid_do_probe() • tests: add functions for work withdisk images • mount: fix undefined reference to `security_get_initial_context'. gentoo: #270168 • libuuid: import UUID library from e2fsprogs • libuuid: add --disable-libuuid and LIBUUID_VERSION • libuuid: add info about u-l-ng to man pages • libblkid: update man page • build-sys: add UTIL_{SET,RESTORE}_FLAGS • build-sys: fix headers in mkswap and libblkid • build-sys: cleanup libuuid stuff • mount: (and fsck) remove libvolume_id support • build-sys: add --disable-libblkid, remove volume_id support • build-sys: enable fsck by default • build-sys: add --disable-tls • uuidgen: new command (from e2fsprogs)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• libuuid: add .gitignore • uuidd: new command (UUID daemon from e2fsprogs) • build-sys: add --disable-uuidd • tests: fix 'delete extended partition' checksum • libblkid: fix reiserfs name • tests: add mdraid libblkid test • tests: fix reiserfs test • tests: don’t run some mount tests for non-root users • tests: remove broken Xen dumps for lscpu • tests: move lscpu /proc and /sys dumps to tarballs • tests: fix script that creates lscpu dumps • docs: add missing commands/projects to AUTHORS file • mount: use TAG parsing function from libblkid • losetup: add --set-capacity • mount: cleanup notes about -l option in mount.8 • mount: add ext4 to mount.8 • mount: add ext4 to the list of filesystems in mount.8 • mount: use "none" fstype for MS_PROPAGATION mounts • mount: move MS_{PROPAGATION,BIND,MOVE} detection • libblkid: don’t require udev symlinks verification for non-root users	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- switch_root: new command - build-sys: add --disable-switch_root - switch_root: fix coding style - switch_root: rewrite to use fstatat() and unlinkat() - build-sys: check for openat() and linux for switch_root - switch_root: use err.h, clean up return codes - switch_root: clean up argv[] usage, add -h and -V - switch_root: use snprintf() rather tan str{cpy,cat}() - switch_root: add man page - docs: refresh TODO list - docs: remove obsolete information from fstab example. - umount: clean up help output. - mount: add info about obsolete vfat options to mount.8. - losetup: suggest to use modprobe rather than insmod in losetup.8. - mount: a little clean up info about loopdevs in man page. - build-sys: fix libuuid Makefile.am - docs: update AUTHORS file - build-sys: fix --disable-uuidd - docs: add v2.16 ReleaseNotes - docs: update v2.16-ReleaseNotes - build-sys: release++ (v2.16-rc1)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• uuidd: move uuidd files from /var/lib/libuuid to /var/run/uuidd • libuuid: move clock state file from /var/lib to /var/run • losetup: fix return codes of functions arounf is_associated() • include: clean up *PATH_DEV** macros • Revert "libuuid: move clock state file from /var/lib to /var/run" • libblkid: fix #ifdefs readability • libuuid: add install-hook for libuuid.[a,so] devel files • libblkid: add install-hook for libuuid.[a,so] devel files • buildsys: move $usr{bin,sbin,lib}execdir definition to ./configure • libblkid: fix $libdir in blkid.pc • libuuid: fix $libdir in uuid.pc • docs: remove example.files/rc[.local] • uuidd: move uuidd.rc to misc-utils directory • uuidd: fix $PIDFILE in uuidd.rc • uuidd: init /var/run/uuidd, add option for on-demand mode to .rc file • include: fix _PATH_DEV • raw: undeprecate raw • blkid: move to misc-utils/ directory • docs: update AUTHORS file	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• docs: update v2.16 ReleaseNotes • build-sys: release++ (v2.16-rc2) • build-sys: fix exec/data install hooks • build-sys: improve symlinks creation in shlibs/ • build-sys: rename to _execdir • libuuid: fix parallel building • build-sys: improve $libdirname definition • libblkid: add stdarg.h to blkidP.h • build-sys: fix libuuid and libblkid version-info • docs: update AUTHORS file • libuuid: generate uuid_generate_{random,time}.3 man page links • docs: update v2.16 ReleaseNotes • build-sys: release++ (v2.16) • po: refresh POTFILES.in • po: merge changes • raw: Use the RAW_SETBIND ioctl without stat'ing the raw# file • switch_root: use file descriptor instead of path for recursiveRemove() • switch_root: fork before cleaning up the filesystem. • switch_root: do recursiveRemove after our root is moved to avoid races. • mount: allow loop suid umount. suse: #461732	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• build-sys: reverse shlibs installation • switch_root: add subroot support • fdisk: (and cfdisk) fix to be consistent about maximum heads • fdisk: add simple test for doslabel stuff • blkid: fix LVM1 probe • blkid: add device-mapper snapshot cow device probe • mount: when a remount to rw fails, quit and return an error • build-sys: fix typo from 30688dde55f637c9b984809c685b61378b82805f • cal: uClibc has langinfo.h but not _NL_TIME_WEEK_1STDAY. • ldattach: add N_PPS support • lscpu: fix cpuid code on x86/PIC • losetup: handle symlinks in /dev/loop/ • build libblkid binary packages • build libuuid binary packages • libuuid: Make sure fd's 0, 1, and 2 are valid before exec'ing uuidd • uuidd: Avoid closing the server socket when calling create_daemon() • libuuid, uuidd: Avoid infinite loop while reading from the socket fd • libuuid: Don't run uuidd if it would fail due to permission problems	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- po: fix typo in French translation. mandriva: #42783 (Olivier Blin) - po: update fi.po (from translationproject.org) (Lauri Nurmi) - po: update fr.po (from translationproject.org) (Nicolas Provost) - po: update vi.po (from translationproject.org) (Clytie Siddall) - po: update cs.po (from translationproject.org) (Petr Pisar) - chrt: don’t assume SCHED_BATCH and SCHED_IDLE exist - remaining kFreeBSD hackery for building. - metafile changes for kFreeBSD buildability hackery. - lscpu: fix cpuid code on x86/PIC - losetup: handle symlinks in /dev/loop/ - Add keybuk as uploader. - meta: cleanup rules targets - hwclock: only call --systz from the udev rule - hwclock: make start a no-op when udev is running - rules: Install udev rules into /lib/udev/rules.d - fdisk: (and cfdisk) fix to be consistent about maximum heads - cal: Highlight today even when month or year specified - cal: uClibc has langinfo.h but not _NL_TIME_WEEK_1STDAY.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• build-sys: fix "make -C" bug • build-sys: fix blkid.h include for old e2fsprogs • blkid: make libuuid optional • blkid: fix "hangs forever with partition type mdraid" • blkid: blkid_do_safeprobe() has to be tolerant to RAIDs • blkid: cleanup debug messages and return codes in blkid_do_probe() • mount: fix undefined reference to `security_get_initial_context'. gentoo: #270168 • libblkid: update man page • libblkid: fix reiserfs name • build-sys: add UTIL_{SET,RESTORE}_FLAGS • build-sys: fix blkid detection in configure.ac • tests: add mdraid libblkid test • tests: fix reiserfs test • tests: don’t run some mount tests for non-root users • tests: remove broken Xen dumps for lscpu • tests: move lscpu /proc and /sys dumps to tarballs • tests: fix script that creates lscpu dumps • docs: update AUTHORS file • docs: add v2.15.1 ReleaseNotes • docs: add missing commands/projects to AUTHORS file • build-sys: release++ (v2.15.1-rc1)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- mount: use "none" fstype for MS_PROPAGATION mounts - mount: move MS_{PROPAGATION,BIND,MOVE} detection - docs: update v2.15.1 ReleaseNotes - build-sys: release++ (v2.15.1) - po: merge changes - po: update vi.po (from translationproject.org) (Clytie Siddall) - chrt: don't assume SCHED_BATCH and SCHED_IDLE exist - kFreeBSD hackery for building. - lscpu: fix cpuid code on x86/PIC - losetup: handle symlinks in /dev/loop/ - Add keybuk as uploader. - fdisk: (and cfdisk) fix to be consistent about maximum heads - cal: Highlight today even when month or year specified - cal: uClibc has langinfo.h but not _NL_TIME_WEEK_1STDAY. - build-sys: fix "make -C" bug - build-sys: fix blkid.h include for old e2fsprogs - blkid: make libuuid optional - blkid: fix "hangs forever with partition type mdraid" - blkid: blkid_do_safeprobe() has to be tolerant to RAIDs	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• blkid: cleanup debug messages and return codes in blkid_do_probe() • mount: fix undefined reference to `security_get_initial_context'. gentoo: #270168 • libblkid: update man page • libblkid: fix reiserfs name • build-sys: add UTIL_{SET,RESTORE}_FLAGS • build-sys: fix blkid detection in configure.ac • tests: add mdraid libblkid test • tests: fix reiserfs test • tests: don’t run some mount tests for non-root users • tests: remove broken Xen dumps for lscpu • tests: move lscpu /proc and /sys dumps to tarballs • tests: fix script that creates lscpu dumps • docs: update AUTHORS file • docs: add v2.15.1 ReleaseNotes • docs: add missing commands/projects to AUTHORS file • build-sys: release++ (v2.15.1-rc1) • po: merge changes • po: update vi.po (from translationproject.org) (Clytie Siddall) • chrt: add a comment about non POSIX 1003.1b attributes in chrt.1 • agetty: IUCLC and OLCUC are Linux extensions	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• blkid: remove whole-disk entries from cache when partitions are found • docs: add a note about /proc/sys/kernel/random/uuid • ionice: change Jens Axboe’s email • losetup: mount endless loop hang. novell: #449646 • cfdisk: fix "cannot seek on disk drive" bug. • blkid: split SONAME and LIBBLKID_VERSION • blockdev: fix possible buffer overflow • fdisk: fix max. ptname • sfdisk: fix possible buffer overflow • docs: add entry about /proc/partitions parsing • blkid: rename blkid_evaluate_spec to blkid_evaluate_tag • tests: fix -regex in run.sh • blkid: linux_raid - fix logic for volumes with size == 0 • blkid: use /dev/mapper/<name> rather than /dev/dm-<N>. red: #497259 • blkid: use /sys/block/dm-<N>/dm/name • docs: update AUTHORS file • docs: update v2.15 ReleaseNotes • build-sys: release++ (v2.15) • po: merge changes • po: update fr.po (from translationproject.org) (Nicolas Provost)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- po: update cs.po (from translationproject.org) (Petr Pisar) - po: update id.po (from translationproject.org) (Arif E. Nugroho) - lib: do not include <linux/fd.h> in ismounted.c - Package - mount: Add strictatime support - blkid: add ZSF support - blkid: fix exit codes in blkid(8) - hwclock: pass --noadjfile if /etc/adjtime not writable - hwclock: always pass --rtc to hwclock calls - blkid: check idinfo[] index - blkid: add ZSF test - blkid: update TODO - blkid: add TODO note about blkid_evaluate_spec_to_buffer() - blkid: add new requirements to TODO list - login: use open(2) rather then access(2) for $HOME/.hushlogin - docs: update AUTHORS file - blkid: add tst_types.c to Makefile.am - docs: update v2.15 ReleaseNotes - build-sys: release++ (v2.15-rc2) - blkid: rename blkid_debug_init to blkid_init_debug	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- po: merge changes - fdisk: suggest partprobe(8) and kpartx(8) when BLKRRPART failed - mkfs.cramfs: lower memory requirements for layouts with duplicate files - hwclock: omit warning about drift if --noadjfile given - mount: retry on ENOMEDIUM - lscpu: return EXIT_SUCCESS at the end - fdisk: add some missing includes - mkfs.minix: fix size detection - cfdisk: accept yes/no as fallback - losetup: try to set up loop readonly if EACCES - include: move swapheader.h to include - swapon: add swap format detection and pagesize check - Disable the fallback clause in hwclock when /dev/rtc cannot be opened. LP: #274402 - hwclock: unshadow a diagnostic printf - hwclock: delay loop in set_hardware_clock_exact - mount: sundries.h add klibc support - mount: s/MOUNTED/_PATH_MOUNTED/ - disk-utils: s/MOUNTED/_PATH_MOUNTED/ - dmesg: nuke old glibc 5 support - misc-utils: write include signal.h directly	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• whereis: include dirent.h instead sys/dir.h • disk-utils: include fcntl.h directly (mkfs.cramfs, raw) • fdisk: exit(3) needs stdlib.h include • remove CVS keywords • mount: add shortoptions for bind, move and rbind • use getpagesize() • partx: don't redeclare daddr_t • sfdisk: fix Compilation Error • rtcwake: support not suspending • ionice: Extend the man page to explain the "none" class and cpu-nice inheritance • build-sys: add --disable-mount • dmesg: Add -r (raw) option. • hwclock: remove x86_64-specific bogon • mount: add norealtime to mount.8 • hwclock: always reads hardware clock. • mount: warn on "file_t" selinux context. red: #390691 • selinux: is_selinux_enabled() returns 0, 1 and -1 • umount: improve "-d" option for autoclear loops • losetup: clean up code around LO_FLAGS_AUTOCLEAR • write: doesn't check for tty group. red: #454252 • build-sys: cleanup sys-utils/Makefile.am	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• mount: make file_t SELinux warning optional and shorter • mount: add info about tz=UTC option for FAT to mount.8 • losetup: looplist_* refactoring, remove scandir() • rtcwake: cleanup return codes • hwclock: cleanup help output and man page • mount: add docs about utf8=0 for vfat. red: #454354 • hwclock: use carefully synchronize_to_clock_tick() return codes • hwclock: use time limit for synchronization busy wait • hwclock: read_hardware_clock_rtc() need to return error codes • scriptreplay: new implementation is out-of-sync • ionice: cleanup man page • ionice: cleanup error messages, add NLS support • docs: TODO update • tests: detect libvolume_id when mount(8) is compiled • fdisk: remove obsolete information from man page • hwclock: don’t open /dev/rtc repeatedly • swapon: -a has to complain, fix leaks • fdisk: warn users about 2.2TB dos partition limit • fdisk: don’t check for GPT when asked for disk size only • fdisk: round reported sizes rather than truncate	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• losetup: remove dependence on minor numbers • login: fix warning "dereferencing type-punned pointer will break strict-aliasing rules" • ionice: add strtol() checks, cleanup usage text and man page • ipcmk: fix error codes and error messages • ipcmk: add NLS support • build-sys: add -luuid to BLKID_LIBS • chrt: add NLS support, clean error messages and return codes • mount: fix typo • mount: add info about /proc/mounts to mount.1 • fsck.cramfs: fix compiler warning • login: fix compiler warning (int32 time() arg) • losetup: missing EBUSY error hint message • mount: mtab created multiple times with -a option • mount: remove link to namesys.com • mount: sync FAT info in mount.8 with Documentation/filesystems/vfat.txt • mount: sync tmpfs info in mount.8 with Documentation/filesystems/tmpfs.txt. red: #465761 • ipcs: fix exit codes, remove tailing white-spaces. red: #465911 • hwclock: remove "cli" and "sti" from i386 CMOS code • docs: update TODO list	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• lscpu: add Hypervisor detection • tests: add mk-lscpu-input.sh • tests: add lscpu(1) test for paravirt. Xen i386 • tests: add lscpu(1) test for fullvirt. Xen x86_64 • tests: refresh Makefile.am (add missing lscpu tests) • fdisk: cannot create partition with starting beyond 1 TB • fdisk: read /proc/partitions in more robust way • fdisk: support +cylinder notation • namei: new re-written version • namei: add --owners and --long options • losetup: add warning about read-only mode • build-sys: move pivot_root(8) to sys-utils • pivot_root: clean up • tests: update namei reg.test • fdisk: fix man page typo • tools: add checkincludes.pl (from linux kernel) • tools: rename codecheck-config to checkconfig.sh • tools: add checkconfig to top-level Makefile • fdisk: rename ENABLE_CMDTAGQ macro • getopt: remove unnecessary ifdefs • hwclock: clock.h is included more than once	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• agetty: sys/types.h and time.h are included more than once • login: cleanup includes • rdev: cleanup includes • tailf: unistd.h is included more than once • mount: add i_version support • mount: reorder list of options in mount.8 • mount: create separate section for fs-independent options in mount.8 • mount: use subsections in mount.8 DESCRIPTION • docs: add feature-requests from RH bugzilla to TODO list • setterm: fix -blank man page • build-sys: add missing AC_C_BIGENDIAN • mkfs.minix: (and fsck) rename bitops.h • include: swapheader.h is missing in Makefile.am • tests: add swabN() regression test • tests: add MD5 regression test • lib: add __BYTE_ORDER to md5.c • include: use __BYTE_ORDER rather than AC specific WORDS_BIGENDIAN • tests: add md5 regression test • mount: fix mount_static_LDADD • Revert "login-utils: several strings without gettext calls"	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• TODO: add request to use nl_langinfo() • chfn: several strings without gettext calls • simpleinit: cleanup gettext calls, use snprintf() • refresh gitignore • pg: add gettext call for the help string • fdisk: remove unnecessary gettext call • mount: clean up SPEC canonicalization • mount: add rootcontext= SELinux mount option • raw: default to /dev/raw/rawctl • namei: fix buffer overflow • mount: add info about semantics of read-only mount to mount.8 • mount: suggest to use blockdev --setro rather than losetup • mount: finalize support of quoted LABELs/UUIDs • umount: cleanup gefs_by_specdir() • ionice: a little cleanup of "none" description • namei: don’t duplicate '/' directory • rtcwake: explain supported modes in rtcwake.8 • namei: add --vertical option • namei: add missing options to namei.1 • rtcwake: add mising .RE to the man page • mount: fix typo in volume_id code	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• ionice: fix typo in manpage • chrt: output buglet when reporting scheduling class • fdisk: add 0xaf HFS / HFS partition type • mount: non-setuid (POSIX file capabilities) support • tests: check also for /dev/loop/X • fsck.cramfs: segfault with INCLUDE_FS_TESTS and no -x option • docs: add suggestion about TZ=UTC to TODO file • mkfs.minix: add regression test • fsck.minix: add regression test • mkfs.minix: remove local implementation of {set,clr}bit • agetty: check for termios.c_line struct member by autoconf • fdisk: cleanup *PATH_DEV** macros • blkid: create basic directories • build-sys: define libdir • blkid: add basic configure.ac stuff and blkid.pc • blkid: merge libblkid code from e2fsprogs/lib/blkid • blkid: minor changes to library build system • blkid: add low level probing API • blkid: add adaptec raid • blkid: optimize for string UUIDs • blkid: add DDF raid	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• blkid: add ISW raid • blkid: add JMicron RAID • blkid: LSI MegaRAID • blkid: NVIDIA raid • blkid: Promise raid • blkid: add Silicon Image Medlay RAID • blkid: add VIA RAID • blkid: update gitignore • blkid: add Linux RAID • blkid: blkdev size fallback • blkid: correctly initialize magics[] arrays • blkid: add ext{2,3,4,4devel} support • blkid: add jfs • blkid: add blkid_probe_get_sb() macro • blkid: add xfs • blkid: fix ext2 SEC_TYPE • blkid: fix xfs label • blkid: add GFS and GFS2 • blkid: add romfs • blkid: add ocfs and oracleasm • blkid: add *attribute* format	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• blkid: fix blkid_probe_sprintf_version() usage • add reiser and reiser4 • blkid: add HFS and HFS+ • blkid: add GFS2 UUID support • blkid: add HTFS • blkid: add missing hfs.c • blkid: add iso9600 • blkid: add LVM2 support and a fix _sprintf_uuid() bug • blkid: add UDF support • blkid: add VFAT support • blkid: re-order list of filesystems • blkid: add LUKS support • blkid: support detection of multiple signatures • blkid: add version and probe FSInfo • blkid: add highpoint{37x,45x} RAIDs • blkid: add lvm1 • blkid: add vxfs • blkid: add minix • blkid: add UFS • blkid: remove unused stuff from Makefile • blkid: add proper copying info	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• blkid: add TODO file • blkid: add HPFS • blkid: cleanup starts of probing files • blkid: fix highpoint37x offset • blkid: use posix uint32_t in ocfs superblock • blkid: use posix uintXX_t in lvm code • blkid: fix hedeader in ntfs.c • blkid: remove blkid_types.h • blkid: add squashfs • blkid: add netware (NSS) • blkid: add sysv and xenix • build-sys: remove use of devmapper library • blkid: use Requires.private and fix the include directory • blkid: fix file descriptor leak when checking for a module • blkid: remove unnecessary ifdef __cplusplus • blkid: add btrfs support • blkid: add DEBUG_LOWPROBE, cleanup a little debug stuff • blkid: add -p and low-probe mode to blkid binary • blkid: add udev string encoding routines • blkid: add udev ID_FS_* output to blkid binary • blkid: refresh TODO file	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• blkid: use sizeof() for hfs uuid • blkid: refresh TODO file • tests: create subdirs for test scripts • tests: remove input directory • tests: create expected/$(component)/$(testname) • tests: add support for subdirs to basic test functions • tests: add ./run.sh <component> • tests: fix TS_* paths • tests: cleanup ts/cal scripts • tests: cleanup ts/col scripts • tests: cleanup ts/hwclock • tests: cleanup ts/ipcs • tests: cleanup ts/login • tests: cleanup ts/look • tests: cleanup ts/namei • tests: cleanup ts/paths • tests: cleanup ts/script • tests: cleanup ts/swapon • tests: cleanup ts/mount • tests: fix output string • tests: add "byte-order" to helpers/test_sysinfo	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- tests: move some generic stuff from ts_init() to a new ts_init_env() - tests: add support for subtests - tests: fix the final message for subtests - tests: add libblkid regression tests (images from e2fsprogs) - blkid: add a note to TODO list - blkid: fix blkid_safe_string() - tests: remove unexpected exit from *_subtest functions - blkid: fix udev output - blkid: add hpfs regression test - blkid: netware SB has to be packed - blkid: add netware regression test - blkid: set size for non-blkdevs, add blkid_probe_strcpy_uuid() - blkid: improve ddf detection - blkid: use blkid_probe_strcpy_uuid() for luks - blkid: remove unnecessary debug message - blkid: fix blkid_do_probe() - blkid: add ddf raid regression test - blkid: fix …_strncpy_uuid - blkid: add ocfs2 version - blkid: add to reiser	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• blkid: add vol_id call to blkid regression test • blkid: add reg.tests for HFS and HFS+ • blkid: add uuid and version support to gfs2 • blkid: add GFS2 reg. test • blkid: add version support to LVM2 • blkid: add lvm2 reg.test • blkid: add blkid_do_safeprobe() • blkid: cleanup _LOGPROBE debug messages • tests: fix typo in low-probe test • blkid: refresh TODO file • blkid: add new options to blkid.8 and help output • blkid: add support for /etc/blkid.conf file • blkid: compile TEST_PROGRAMs • blkid: fix typo (syntax error) • mount: move realpath.c code to lib/ • blkid: add blkid_evaluate_spec() • blkid: clean up man pages • blkid: refresh TODO file • blkid: add findfs(8) • build-sys: add --with=fsprobe=builtin • blkid: start to use ABI versioning	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• build-sys: libtoolize by libtool-2 • build-sys: libtoolize mount/Makefile.am • build-sys: add temporary libtool *.m4 stuff • blkid: refresh TODO file • blkid: add Christoph’s note about libdisk to TODO • mount: generic blkid/volume_id wrapper, use blkid_evaluate_* • build-sys: use pkg-config for blkid and volume_id • blkid: add TODO hint about DM devnames in sysfs • blkid: check calloc() return value • blkid: add cmdline interface for blkid_probe_filter_usage() • blkid: add TODO hint about blkid_parse_tag_string() • blkid: fix low-probe mode return codes • fsck: move fsck from e2fsprogs to util-linux-ng • lib: make open_device() optional in fsprobe.c • fsck: link with generic fsprobe wrapper • fsck: cosmetic changes (NLS, paths, …) • lib: add test_ismounted for regression test • tests: add fsck:ismounted reg.test • tests: cleanup ts/bitops • tests: cleanup ts/cramfs/fsck-endianness • tests: cleanup ts/cramfs/mkfs-endianness	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• tests: cleanup lscpu reg.tests • build-sys: add fsck binary to .gitignore • tests: cleanup ts/minix • tests: cleanup ts/md5 • tests: chmod -x ts/lscpu/mk-input.sh • tests: we needn’t blkid.sh • tests: refresh cal(1) expected outputs • tests: refresh ipcs expected outputs • blkid: blkid_evaluate_spec() shouldn’t ignore $BLKID_FILE • mount: inform about UID and eUID when verbose > 2 • tests: disable suid mount test • tests: refresh expected mount(8) outputs • losetup: detach more devices by "-d <loop> [<loop> ..]" • losetup: cleanup man page • tests: remove obsolete stuff from Makefile.am • fsck: remove \007 from warning message • build-sys: add missing files to include/Makefile.am • blkid: fix a syntax nit • fsck: remove useless if-before-free tests • getopt: remove useless if-before-free tests • mount: remove useless if-before-free tests	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• fdisk: use real sector size in verify() and warn_cylinders() • blockdev: add note that the StartSec is in 512-byte sectors • addpart: 512-byte sectors in code, bytes in man-page • partx: convert hard sector size to 512-byte sectors • partx: don’t duplicate lib/blkdev.c code • fdisk: (and partx) remove BLKGETLASTSECT • partx: use ioctls from lib/blkdev.c • docs: add a note about kpartx to TODO • swapon: do_swapon() refactoring (move stat() checks) • swapon: add generic swap_get_header() • swapon: simplify spec to devname conversion • swapon: use err.h stuff • swapon: do_swapon() refactoring (split into two functions) • swapon: rewrite SWSUSPEND signature rather than exec mkswap • swapon: cleanup man page • swapon: add -f/--fixpgsz option • simmpleinit: fix gcc warning (buffer size in read()) • mount: fix gcc warning (variable used uninitialized) • blkid: use "char **" rather than "unsigned char** " • blkid: fix gcc warning in blkid_get_cache_filename()	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• lib: gcc warning in fix fsprobe • lib: fix fsprobe wrapper (const char * is nonsense) • swapon: fix wording in man page • swapon: fix typo s/warn/warnx/ • swapon: add error messages for lseek and write • login: remove "switching users" nonsense from man page • fdisk: support "-b 4096" option • blkid: blkid.static make target • build-sys: cleanup --with-fsprobe help string • renice: add -n option for compatibility with POSIX • cal: remove gcc-ism from nl_langinfo() call • flockc: segfaults when file name is not given. red: #489672 • flock: fix printf format error in usage() • flock: add NLS support, remove tailing white-spaces • lib: add is_whole_disk() from fdisk code • mkswap: remove v0 swap space support • lib: add pttype.c for PT types detection • include: add missing files to Makefile.am • lib: pttype: add BSD subpartitions support • lib: pttype: fix DOS detection • lib: pttype - extend the API to work with file descriptors	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• lib: wholedisk - extend API, add test program • libs: pttype - fix typo • mkswap: zap bootbits • mkswap: clean up man page • blkid: fix non-udev low-probe mode output • lib: fsprobe - fix gcc warning • tests: disable blkid tests when blkid(8) is not compiled • blkid: add missing blkidP.h to Makefile.am • build-sys: refresh generated libtool-2 stuff • include: bitops - explicitly include endian.h • build-sys: add $usrlibexecdir and fix paths for [/usr]/lib64 • blkid: fix ocfs2 detection • login: use "remote" as a PAM service name for "login -h" • tests: fix file name is too long (max 99) - gtar • tests: fix typo in lscpu test • docs: update AUTHORS file • docs: update v2.15 ReleaseNotes • build-sys: fix bugs detected by "make distcheck" • build-sys: release++ (v2.15-rc1) • docs: fix typo, cal(8) -→ cal(1) • po: update list of .c files	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- po: merge changes - po: update POTFILES.in - po: rewrite update-potfiles script - elvtune: add NLS support - fsck.cramfs: add NLS support - mkfs.cramfs: several strings without gettext calls - raw: add NLS support - fdisk: several strings without gettext calls - hwclock: several strings without gettext calls - login-utils: several strings without gettext calls - logger: several strings without gettext calls - losetup: several strings without gettext strings - readprofile: several strings without gettext calls - pg: several strings without gettext calls - more: minor fixes to magic() - mount: document newinstance and ptmxmode options to devpts - hwclock: add --systz option to set system clock from itself - debian/control: Add build-dependency on pkg-config - umount: check for overlaid mounts - mount: fix typo - ipcmk: new command	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Fix dmesg.1 installation • flock: Allow lock directory • blkis: fix detection of ext4dev as ext4 • blkid: recognize ext3 with test_fs set as ext3 • fdisk: doesn’t handle large (4KiB) sectors properly • blkid: recognize ext4(dev) without journal • blkid: vfat - fix declaration • blkid: hfs - use proper native UUID format • blkid: hfs - do not set UUID for emtpy finder info • lscpu: new command • lscpu: --sysroot option and stable cache output • lscpu: regression tests • ionice: let -p handle multiple PIDs • blkid: don’t dereference NULL upon slashless module dependency line • blkid: remove useless if-before-free tests • mount: cleans up mount(8) troff markup • tests: clean up the testing scripts • tests: remove useless return value checks in testing scripts • blkid: support via raid version 2 • mkfs.cramfs: add endianness support to cramfs tools	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• chrt: support CFS SCHED_IDLE priority and document it • mkswap: non-linux support • fdisk: don’t use get_linux_version() for non-linux • lib: blkdev.c clean up, non-linux support • fdisk: non-linux support (BLK* and HDIO_*) • disk-utils: clean up code, use blkdev_* functions • ldattach: don’t compile for non-linux systems • ipcs: ungettextize the spacing of the table headers • ipcs: adjust some field positions and widths for correct alignment • po: update nl.po (from translationproject.org) • sfdisk: print version should end with a newline • build-sys: tgets is not in ncurses but in tinfo • rtcwake: prefer RTC_WKALM_SET over RTC_ALM_SET • more: dont use a.out.h • mount: remove spurious newline from mount.8 • ionice: add -t option. red: #443842 • blkid: Optimize devicemapper support • blkid: Unexport the private symbol blkid_devdirs • blkid: Give a priority bonus to "leaf" devicemapper devices • blkid: Refuse to create a device structure for a non-existent device.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• blkid: add fallback to ext4 for 2.6.29+ kernels if ext2 is not present • umount: no checking mount point removal • mkswap: handle 2^32 pages • script: don't flush input when starting script • tests: refresh and cleanup cramfs/mkfs • blkid: add -L -U options (evaluation API) • cal: determine the first day of week from the locale • po: update id.po (from translationproject.org) (Arif E. Nugroho) • po: update ja.po (from translationproject.org) (Makoto Kato) • po: update cs.po (from translationproject.org) (Petr Pisar) • po: add zh_CN.po (from translationproject.org) (Ray Wang) • po: update fr.po (from translationproject.org) (Nicolas Provost) • po: update vi.po (from translationproject.org) (Clytie Siddall) • po: update fi.po (from translationproject.org) (Lauri Nurmi) • mount: segfault when creating mtab and cannot determine fsname. • hwclockfirst.sh: use correct LSB header info. • chrt: output buglet when reporting scheduling class • mount: fix typo in volume_id code	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• docs: update AUTHORS file • docs: update v2.14.2 ReleaseNotes • build-sys: release++ (v2.14.2) • po: merge changes • po: update vi.po (from translationproject.org) (Clytie Siddall) • po: update cs.po (from translationproject.org) (Petr Pisar) • po: update ja.po (from translationproject.org) (Makoto Kato) • po: update nl.po (from translationproject.org) (Benno Schulenberg) • hwclock: omit warning about drift if --noadjfile given • cfdisk: accept yes/no as fallback • fdisk: add some missing includes • losetup: try to set up loop readonly if EACCES • mkfs.minix: fix size detection • mount: retry on ENOMEDIUM • hwclock: unshadow a diagnostic printf • mount: sundries.h add klibc support • use getpagesize() • ionice: Extend the man page to explain the "none" class and cpu-nice inheritance • hwclock: remove x86_64-specific bogon	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• mount: add norealtime to mount.8 • selinux: is_selinux_enabled() returns 0, 1 and -1 • umount: improve "-d" option for autoclear loops • write: doesn’t check for tty group • rtcwake: cleanup return codes • mount: add info about tz=UTC option for FAT to mount.8 • build-sys: cleanup sys-utils/Makefile.am • build-sys: fix dmesg.1 installation • mount: add fallback for versionsort() • mount: add docs about utf8=0 for vfat • scriptreplay: new implementation is out-of-sync • docs: update AUTHORS file • docs: update v2.14.1 ReleaseNotes • build-sys: release++ (v2.14.1-rc1) • losetup: remove unnecessary minor number check • fdisk: don’t check for GPT when asked for disk size only • docs: update AUTHORS file • docs: update v2.14.1 ReleaseNotes • build-sys: release++ (v2.14.1-rc2) • docs: update v2.14.1 ReleaseNotes • build-sys: release++ (v2.14.1)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- mount: mtab created multiple times with -a option - build-sys: add -luuid to BLKID_LIBS - lib: add __BYTE_ORDER to md5.c - include: use __BYTE_ORDER rather than AC specific WORDS_BIGENDIAN - fdisk: cannot create partition with starting beyond 1 TB - fdisk: remove obsolete information from man page - fdisk: fix man page typo - fdisk: support +cylinder notation - hwclock: remove "cli" and "sti" from i386 CMOS code - login: fix warning "dereferencing type-punned pointer will break strict-aliasing rules" - login: fix compiler warning (int32 time() arg) - losetup: add warning about read-only mode - losetup: missing EBUSY error hint message - mount: add info about /proc/mounts to mount.1 - mount: add i_version support - mount: reorder list of options in mount.8 - mount: sync FAT info in mount.8 with Documentation/filesystems/vfat.txt - mount: sync tmpfs info in mount.8 with Documentation/filesystems/tmpfs.txt - mount: remove link to namesys.com	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• mount: create separate section for fs-independent options in mount.8 • mount: fix typo • mount: use subsections in mount.8 DESCRIPTION • mount: warn on "file_t" selinux context • mount: make file_t SELinux warning optional and shorter • setterm: fix -blank man page • mount: fix mount_static_LDADD • fdisk: remove unnecessary gettext call • refresh gitignore • docs: update AUTHORS file • mount: clean up SPEC canonicalization • mount: add rootcontext= SELinux mount option • docs: update v2.14.2 ReleaseNotes • build-sys: release++ (v2.14.2-rc1) • mount: add info about semantics of read-only mount to mount.8 • mount: suggest to use blockdev --setro rather than losetup • mount: finalize support of quoted LABELs/UUIDs • ionice: a little cleanup of "none" description • docs: update AUTHORS file • docs: update v2.14.2 ReleaseNotes	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• build-sys: release++ (v2.14.2-rc2) • po: merge changes • fdisk: several strings without gettext calls • logger: several strings without gettext calls • losetup: several strings without gettext strings • mkfs.cramfs: several strings without gettext calls • readprofile: several strings without gettext calls • mount: cleans up mount(8) troff markup • mount: fix typo • build-sys: tgets is not in ncurses but in tinfo • rtcwake: prefer RTC_WKALM_SET over RTC_ALM_SET • chrt: support CFS SCHED_IDLE priority and document it • ldattach: don’t compile for non-linux systems • ipcs: ungettextize the spacing of the table headers • po: update nl.po (from translationproject.org) • sfdisk: print version should end with a newline • more: dont use a.out.h • mount: remove spurious newline from mount.8 • more: minor fixes to magic() • po: update id.po (from translationproject.org) (Arif E. Nugroho)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• po: update pt_BR.po (from translationproject.org) (Rodrigo Stulzer Lopes) • po: update zh_CN.po (from translationproject.org) (Ray Wang) • po: add zh_CN.po (from translationproject.org) (Ray Wang) • po: update sv.po (from translationproject.org) (Daniel Nylander) • po: update fr.po (from translationproject.org) (Nicolas Provost) • po: update vi.po (from translationproject.org) (Clytie Siddall) • po: update cs.po (from translationproject.org) (Petr Pisar) • po: update fi.po (from translationproject.org) (Lauri Nurmi) • rules: drop separate configure target. • ddate: 11th, 12th and 13th of month • rtcwake: fix the default mode to "standby" • mount: fix a small typo in mount.8 • Update menu-item number for Debian Installer components. • docs: update AUTHORS file • docs: update v2.14 ReleaseNotes • build-sys: release++ (v2.14) • po: merge changes • po: update hu.po (from translationproject.org) (Gabor Kelemen)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• lomount: initialize sizelimit (lost in merge). LP: #230974 • meta: fix description of bsdutils. • control: add support for sh4. • docs: we already rewrote the scriptreplay script; remove that TODO entry • setarch: add fallback for linux/personality • fdisk: doesn't recognize the VMware ESX partitions • build-sys: add support ionice for Super-H architecture • mount: remount doesn't care about loop= • po: merge changes ○ po: update cs.po (from translationproject.org) (Petr Pisar) ○ po: update nl.po (from translationproject.org) (Benno Schulenberg) ○ po: update it.po (from translationproject.org) (Marco Colombo) ○ po: update vi.po (from translationproject.org) (Clytie Siddall) • docs: update 2.14 ReleaseNotes • build-sys: release++ • login: audit log injection attack via login • po: merge changes ○ po: update it.po (from translationproject.org) (Marco Colombo)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ po: update nl.po (from translationproject.org) (Benno Schulenberg) • ionice: update man page to reflect IDLE class change in 2.6.25 • scriptreplay: gettextize a forgotten messages • docs: update v2.14 ReleaseNotes • build-sys: release++ • New upstream version • control: drop -1 version from libslang2-dev build-dep • control: standards-version 3.7.3.0 • login: audit log injection attack via login • po: merge changes ○ po: update it.po (from translationproject.org) (Marco Colombo) ○ po: update nl.po (from translationproject.org) (Benno Schulenberg) • docs: add v2.13.1.1 ReleaseNotes • build-sys: release++ (2.13.1.1) • control: drop -1 version from libslang2-dev build-dep • control: standards-version 3.7.3.0 • Switch to upstream’s more-correct fix for LP#206113 • mkswap: when writing the signature page, handle EINTR returns. LP: #206113 • meta: Drop bashism in preinst.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• mkswap: when writing the signature page, handle EINTR returns. LP: #206113 • swapon: Reinitialize software suspend areas to avoid future corruption. LP: #66637 • Add menu item numbers for *fdisk udebs. • agetty: make username-in-uppercase feature optional (off by default.). • debian/rules: allow cross-building. • hwclock.sh: fix typo. LP: #103680 • mkswap: Set UUID for swap space. • mkswap: -U UUID cleanup • New Upstream Release [Karel Zak] ○ docs: update AUTHORS file ○ docs: update ReleseNotes ○ build-sys: release++ (2.13.1) ○ po: merge files ○ po: update uk.po (from translationproject.org) (Maxim V. Dziumanenko) ○ po: update it.po (from translationproject.org) (Marco Colombo) ○ po: update sl.po (from translationproject.org) (Simon Mihevc) ○ po: update ru.po (from translationproject.org) (Pavel Maryanov) ○ po: update cs.po (from translationproject.org) (Petr Pisar)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ po: update pt_BR.po (from translationproject.org) (Rodrigo Stulzer Lopes) ○ po: update id.po (from translationproject.org) (Arif E. Nugroho) ○ po: update es.po (from translationproject.org) (Santiago Vila Doncel) ○ po: update hu.po (from translationproject.org) (Gabor Kelemen) ○ po: update eu.po (from translationproject.org) (Mikel Olasagasti) ○ po: update ca.po (from translationproject.org) (Josep Puigdemont) ○ po: update sv.po (from translationproject.org) (Daniel Nylander) ○ po: update fr.po (from translationproject.org) (Michel Robitaille) ○ po: update tr.po (from translationproject.org) (Nilgün Belma Bugüner) ○ po: update ja.po (from translationproject.org) (Daisuke Yamashita) ○ po: update nl.po (from translationproject.org) (Benno Schulenberg) ○ po: update pl.po (from translationproject.org) (Andrzej Krzysztofowicz) ○ po: update da.po (from translationproject.org) (Claus Hindsgaul)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ po: update vi.po (from translationproject.org) (Clytie Siddall) ○ po: update et.po (from translationproject.org) (Meelis Roos) ○ po: update de.po (from translationproject.org) (Michael Piefel) ○ po: update fi.po (from translationproject.org) (Lauri Nurmi) ● hwclockfirst.sh: yet more tweaks for LSB init. ● meta: mount should pre-depend on its libs ● hwclock.sh: add full path to comment. ● renice: correctly detect errors in arguments. ● docs: update AUTHORS file, add all translators ● docs: update ReleaseNotes ● po: update po files ○ po: update uk.po [Maxim V. Dziumanenko] ○ po: update id.po [Arif E. Nugroho] ○ po: update es.po [Santiago Vila Doncel] ○ po: update hu.po [Gabor Kelemen] ○ po: update it.po [Marco Colombo] ○ po: update sl.po [Simon Mihevc] ○ po: update ru.po [Pavel Maryanov] ○ po: update cs.po [Petr Pisar] ○ po: update pt_BR.po [Rodrigo Stulzer Lopes]	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ po: add eu.po [Mikel Olasagasti] ○ po: update ca.po [Josep Puigdemont] ○ po: update sv.po [Daniel Nylander] ○ po: update fr.po [Michel Robitaille] ○ po: update tr.po [Nilgün Belma Bugüner] ○ po: update ja.po [Daisuke Yamashita] ○ po: update nl.po [Benno Schulenberg] ○ po: add pl.po [Andrzej Krzysztofowicz] ○ po: update da.po [Claus Hindsgaul] ○ po: update vi.po [Clytie Siddall] ○ po: update et.po [Meelis Roos] ○ po: update de.po [Michael Piefel] ○ po: update fi.po [Lauri Nurmi] • build-sys: release++ (-rc2) • mount: hint about helper program if device doesn’t exist. • rules: correct LSB init data for hwclockfirst.sh. • hwclock: check for ENODEV • mount: fix fd leak • sys-utils: Drop duplicate install of setarch manpage links. • agetty: drop useless and unused diff from upstream • hwclock.sh: drop redundant file pointer.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• sys-utils: correct setarch.8 manpage link creation. • build-sys: remove hardcoded _GNU_SOURCE • mount: don’t call canonicalize(SPEC) for cifs, smbfs and nfs. • blockdev: add --getsz to blockdev.8 • meta: drop Conflicts: bsdmainutils too • cal comes from bsdmainutils as well. Drops Replaces: completely. • docs: fix ChangeLog URL • po: update hu.po (from translationproject.org) • losetup: fix errno usage • po: update po files • po: update fi.po (from translationproject.org) • mkswap: possible to crash with SELinux relabeling support • docs: add info about .bugfix releases and branches • build: don’t deliver col* and ul as part of bsdutils for now. • deliver hwclockfirst.sh on ubuntu as well. LP: #63175 • build: don’t deliver (emtpy) /usr/share/util-linux. • mount.8: Make package references be the actual binary package name in the distro. LP: #154399 • po: update de.po (from translationproject.org) • chsh: should use pam_end function to terminate the PAM transaction	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• po: update nl.po (from translationproject.org) • pg: fix segfault on search • mount: -L|-U segfault when label or uuid doesn’t exist • tests: fix blkid cache usage • script: dies on SIGWINCH. • chfn: add pam_end() call and cleanup PAM code • ionice: add a note about permissions to ionice.1 • script: dies on SIGWINCH • po: fix typo in de.po • po: update po files • setarch: generate groff links in a better way • Upstream git: ○ po: update sv.po (from translationproject.org) ○ mount: doesn’t drop privileges properly when calling helpers CVE-2007-5191 ○ hwclock: fix --rtc option. ○ setarch: fix compiler warning ○ login: login segfaults on EOF (rh#298461) ○ build-sys: nls/locale handling in util-linux-ng general ○ blockdev: add missing description about option --report in manpage • fix messages in "hwclock.sh start".	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- Honor DEB_BUILD_OPTIONS=nostrip. - cfdisk.8: mention slang next to curses. - util-linux.postrm: remove /etc/adjtime on purge. - hwclock: Reintroduce hwclockfirst.sh on Debian machines. - mount.preinst: chroot-check was broken. - sparc-utils 'sparc64' binary sets ADDR_LIMIT_32BIT. - build: cfdisk doesn't exist on some architectures. - build: look for fdisk in the right place. - flock.1: typo in man page. - mount: chain of symlinks to fstab causes use of pointer after free - Replaces: sparc-utils (for sparc{32,64}. - Don't make rename.ul an alternative for rename. - Don't deliver hexdump (bsdmainutils is newer). - Update bsdutils description. - Changes from upstream: ○ docs: update AUTHORS file ○ Revert "mount: improve error message when helper program not present" for translation freeze (reopens LP #131367) Will be fixed in 2.13.1 and 2.14. ○ taskset: check for existence of sched_getaffinity ○ setarch: add parisc/parisc64 support	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ mount: free loop device on failure ○ mount: avoid duplicates for root fs in mtab ○ build-sys: release++ ○ docs: update ReleaseNotes, update and sort AUTHORS file ○ po: update po/ stuff ○ ionice: clean up error handling ○ cytune: make the oneliner more specific the cyclades hw in question ○ docs: update TODO ○ setarch: add --3gb option for compatibility with Debian linux{32,64} command • Revert "umount: only call update_mtab if mtab_is_writable().", since the fix is already present in a different way. • Have debian/rules deal with architectures that don't get packages. • debian/rules: cleanup and support nostrip option • build: fdisk (and therefore the udebs) do not get built on m68k. • build: /usr/bin/rename needs to be an alternative. • taskset: Don't deliver taskset on m68k. • umount: only call update_mtab if mtab_is_writable(). • build: switch back to libblkid-dev for Debian. • Document git repository location	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• cytune.8: make the oneliner more specific the cyclades hw in question • control: Extend package descriptions. • Switch to debhelper, clean up delivery of binaries. • bsdutils: deliver more stuff that we build. Now partly Replaces: bsdmainutils and completely Replaces: linux32. • more upstream changes ○ docs: add DEPRECATED to EXTRA_DIST ○ docs: update AUTHORS file ○ docs: add note about http://translationproject.org ○ man-pages: cleanup of chrt.1 and taskset.1 ○ mount: improve error message when helper program not present ○ setarch: cleanup licensing note ○ setarch: add sparc32bash alias to keep compatibility with sparc32 ○ setarch: add *alpha* support ○ po: update de.po, vi.po, nl.po (from translationproject.org) • drop arch.1 man page. • deliver the right file for scriptreplay. • sfdisk: Allow drives over 2^31 sectors in size. • Deliver flock and flock.1. • hwclock.sh: Correct message.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• cfdisk: switch back to slang2 • setarch: add parisc/parisc64 support • deliver setarch • Fix distro check in debian/rules • Use Breaks: on distros that support that in the previous release. • Changes from upstream: ○ po: gettextizing some overlooked messages. ○ build-sys: add --disable-makeinstall-chown ○ docs: add README.licensing ○ tests: fix ULONG_MAX usage on 32bit machines ○ chsh: don’t use empty shell field in /etc/passwd ○ more: fix underlining for multibyte chars ○ login: replace /usr/spool/mail with /var/spool/main in man page • mount: make the error message a little more clear when a helper program is missing. (LP #131367) • manpages: cleanup of chrt.1 and taskset.1. • hwclock.sh: only report hwclock updated if we did that. • update copyright to reflect README.licensing • Merge ubuntu changes, do the right thing at build time. • Go back to Depends: for the various packages, since the switch to libc5 is long, long over.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			● Merge lpia support from ubuntu. ● Add lpia support back in. sorry. ● New debian version. Remaining ubuntu changes: ○ Add udev rule for calling /sbin/hwclock --hctosys dynamically: + debian/hwclock.rules, debian/hwclock.udev: Rule and script. + debian/rules: Install those. ● mount should Suggest nfs-common, not Recommend it. ● Fix build-depends for hurd-i386. ● Merge ubuntu changes into a new Debian version. Remaining: ○ Add udev rule for calling /sbin/hwclock --hctosys dynamically: + debian/hwclock.rules, debian/hwclock.udev: Rule and script. + debian/rules: Install those. ● New upstream version ● If nfs-common is not installed, skip nfs check ● More fixes from upstream: ○ swapon: cleanup fsprobe_*() usage ○ swapoff: correctly handle UUID= and LABEL= identifiers ○ mount: fix incorrect behavior when more than one fs type is ○ tests: add script(1) race condition test ○ script: fix race conditions ○ mkfs: remove nonsense from man page ○ blockdev: use LU and LLU for BLKGETSIZE and BLKGETSIZE64	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ blockdev: fix "blockdev --getsz" for large devices ● Merge ubuntu fixes into new Debian version. ● More fixes from upstream ● mount.preinst: deal with no /proc/mounts. ● swapoff: handle UUID= and LABEL=. ● mount.preinst: ○ check the right directory for mount.nfs. ○ look for ' nfs ' mounts. ● switch to using libvolume-id-dev ● Recommend: nfs-common so that portmap doesn’t become defacto-Required. NFS mounts will not work unless nfs-common is upgraded to at least the Recommended version, so now mount.preinst will fail if there are NFS mounts and no /usr/sbin/mount.nfs. ● Merge ubuntu changes: ○ Add udev rule for calling /sbin/hwclock --hctosys dynamically: + debian/hwclock.rules, debian/hwclock.udev: Rule and script. + debian/rules: Install those. ○ use libvolume-id instead of blkid. This will be true for debian once a current enough udev is available. ● add option for 8-bit chars in agetty. ● Merge upstream fixes (rc2+git) ● arch is dealt with upstream now. ● Mention hfsplus in mount.8. ● Add m32r.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• use snprintf in logger.c. • Various typos in cfdisk.8. • cleanup copyright. • manpage typos. • New upstream version • drop libselinux-dev build-dep on kfreebsd-amd64 • A little more kfreebsd cleanup • Fix nfs-common dependency • fix ionice build errors on several architectures. • no libselinux on kfreebsd-i386 • New upstream (util-linux-ng). ○ several patches were not ported forward from 2.12-19 ○ no kerneli support in crypto loop, since it is not in 2.6 kernels. ○ 20guesshelper: filesystem detection has been dropped. Mount is built with filesystem probing ○ 20xgethostname: does anyone care? ○ 30nfs*: NFS support has moved to nfs-utils, and removed from util-linux. Add Depends: nfs-common until Lenny ships. ○ umounting usb sticks as a user no longer segfaults. • Add LSB formatted dependency info in hwclock.sh. • Reflect Debian locations in getopt manpage.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Conflict/Replaces/Provides: schedutils. • README.Debian.hwclock needs a .gz in hwclock.sh. • Deliver tailf. • Deliver partx. • USB unmounting dereferenced a null pointer. ○ Files: 70fstab.dpatch • Fix sparc disk label generation. This is required for LDOM and parallel installations with Solaris 10. Add patch: 80sparc-new-label Many thanks to David S. Miller for the patch. NOTE: users upgrading from older versions should re-run fdisk to update the disk label. • Merge from debian unstable, remaining changes: ○ Use volumeid instead of blkid to be able to access (mount/umount/swapon) volumes by UUID and/or label: + debian/control: libblkid-dev → libvolume-id-dev build dependency + debian/patches/70libvolume_id-support.dpatch: SuSE patch for using libvolume-id. ○ Add udev rule for calling /sbin/hwclock --hctosys dynamically: + debian/hwclock.rules, debian/hwclock.udev: Rule and script. + debian/rules: Install those. • mips/mipsel buildds use sudo. Fix install target so that mount.deb builds. • Stop printing erroneous "rpc.idmapd appears to not be running" message. Files: 30nfs4.dpatch. • debian/control: Update maintainer fields according to debian- maintainer-field spec. • Merge from Debian unstable. Remaining changes: ○ libvolume_id support patch from SuSE	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ single ubuntuized hwclock script • Userspace software suspend fix. • armel support. • actually apply 30swsusp-resume. And support userspace sw susp too. • Fix off-by-one issue in agetty -I. • Drop extraneous "again" from hwclock.sh and remove references to hwclockfirst.sh. • Drop PAGE_SIZE usage completely, use sysconf(_SC_PAGESIZE). • Make intr the default for NFS v2 & v3 mounts in addition to being the default for NFS v4. Thanks to Tollef Fog Heen for the idea. • New amd64 rdev patch. • Make that 11 for hwclock.sh, since we need / to be writable for the adjfile. • NFS seems to not like 127.0.0.1 as a client ID for everyone. ○ 30nfs4-setclientid.dpatch by Steinar H. Gunderson <sesse@debian.org> • Move hwclock.sh to 8 since localtime is now a file, not a symlink. Adds Depends: tzdata (>=2006c-2) • ship rdev on amd64. • drop hwclockfirst.sh, and put hwclock.sh back at 50. See #50572 and • Deal with _syscall5 going away. Patch imported from Ubuntu. • typos in NFSv4 (GSSDLCK didn't have .pid, and the latest nfs-common no longer creates the file at all.)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ modified 30nfs4-fix.dpatch • NFSv4 patch fixes for cfs. Thanks to Trond Myklebust for the quick fix. ○ modified 30nfs4-fix.dpatch • Release NFSv4 support. • Deliver isosize. • Fix udeb dependencies. • Turn on fixed nfsv4 patch. Thanks to Steinar H. Gunderson <sgunderson@bigfoot.com> • Drop NFS v4 patch, since it breaks mounting things exported by nfs-user-server. It will be happily reapplied once someone fixes the patch. ○ fix compiler warnings in said patch. ○ Apply nfs4mount.c fix to (dropped) nfsv4 patch. • Add nfsv4 patch. • make hwclock even more policy compilant. • make hwclock prettier. • Stupid fat-fingers typo. • Add ppc64 support. • Update sections to match the overrides file. • hwclockfirst.sh may not exit, since it gets sourced. • make the start messages from hwclock{first,}.sh slightly different, for clarity. • Build sparc binaries on sparc64	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Actually cleanup pager alternatives. • Deal better with long passwords. Based on patch from YAEGASHI Takeshi <yaegashi@debian.org>. • Add back in dropped cramfs-udebsize patch. • New upstream verison and maintainer. ○ cfdisk: fix a segfault with ReiserFS partitions ○ umount: disallow -r option for non-root users (CAN-2005-2876) ○ sfdisk: document -G option in --help output ○ updated translations: ca, et, fr ○ sfdisk: add -G option (Andries Brouwer) ○ updated translations: de, es, ru, sv, tr, nl • split cfdisk into its own udeb. • Really move hwclockfirst.sh back to S18 where it belongs. Put hwclock.sh at S22. See #50572. • Missing line break in hwclock.sh. • Include swap-suspend patch from Ubuntu. • Fix variable name typo in hwclock.sh. • Add CPU=$(arch) to make call for building on amd64/i386 mixed systems. • Cleanup lsb_init function usage. • if /etc/adjtime is a dangling symlink, don't use it in hwclock*.sh	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Applited patch by Max Vozeler to fix a local privilege escalation vulnerability in umount -r [debian/patches/51security_CAN-2005-2876.dpatch] • Fix non-posix typo in hwclock.sh. • Use helper program in mount for guessed FS types too. Thanks to Manish Singh and Fabio Massimo Di Nitto. Adds: 20guesshelper.dpatch • Remove /usr/doc links on install. • Fix /usr/bin/pg pager alternative. • Overhaul hwclock.sh and hwclockfirst.sh. • Resync with Ubuntu, changes by Martin.Pitt@ubuntu.com: debian/patches/60_opt_O1.dpatch: ○ MCONFIG, configure: Build with -O1 instead of -O2 to work around cfdisk segfault. ○ Yay for upstream build systems which do not support specifying CFLAGS or OPT without breaking. • Merge changes from ubuntu ○ closes #319143 • Build-Depend: libslang2-dev. • dpkg-architecture says DEB_HOST_GNU_SYSTEM is "linux-gnu" now, not "linux". Take account of this, and add compatibility code for old dpkg-architecture • Don't special case sparc, it has umount2. • Run hwclockfirst.sh after modules load, so that rtc is loaded. • Resynchronise with Debian. • correct shutdown message from hwclock.sh	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- Depend on newer libblkid1. - Add an alternative for pager pointing at pg (at pref 10). - enable fdisk on s390. - Update dependencies for new libblkid1 - Resync with Debian. - Really fix man page in alternatives. - more typos in hwclockfirst.sh. - Resync with Debian. Closes warty #3366, 4784 - New upstream version. (2.12p) ○ cfdisk: fix number of new partition when partitions not in disk order ○ fdisk: fix Sun label handling in sector mode ○ mkfs: never truncate filename (not that that ever happened) ○ more: fix redraw flaw. - New upstream version. (2.12o) ○ lomount: revert patch from 2.12j ○ lptune.8: -T option is obsolete ○ mkswap, mkswap.8, swapon: support labels (use HAVE_BLKID=no as long as the blkid library doesnt support this) ○ umount: allow user unmounting repeatedly mounted nfs mounts - Build-Depend on uuid-dev. - correct chown args in debian/rules.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• include man page in update-alternatives for pager. • fix typos in howclockfirst.sh. • fix losetup -N documentation. • cleanup some narrow window sprintf issues in cfdisk. • Resync with Debian. • New upstream version ○ cfdisk: recognize JFS, support reiserfs labels (flavio.stanchina@tin.it) ○ mount: fix option parsing bug ○ mount.8: several updates ○ swapon.8: document -v option • Resync with debian • New upstream version, shrinking the size of the Debian diff. ○ Makefile: remove cat-id-tbl.c upon make clean ○ fdisk: fixed a bug that would cause a non-update of a sun disklabel ○ fdisk: use sectorsize instead of 512 for SGI (Eric Y. Theriault) ○ fdisk: use *attribute*packed for alpha, ARM: avoid unaligned accesses ○ hwclock: actually use HAVE_tm_gmtoff ○ swapon: fix priority handling ○ umount: refuse to unmount an empty string • Jetisoning the (broken) hurd patch for now.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Resync with Debian • Switch to dpatch. • Clean up --nohashpass in losetup. • Use stat instead of open in losetup. (From #285353) • Resync with Debian • New upstream version. • various translation updates • gcc-3.4 support help • Resync with Debian • umount -l "" does bad things. Don't do let the user do that. • remove non-utf8 characters from changelog. sorry. • resync with Debian • uninitialized variable. • resync with Debian • New upstream version • resync with debian. • mkswap on a file was broken. Thanks to Bas Zoetekouw <bas@debian.org> for the patch. • add libblkid-dev to Build-Depends. • Resync with debian. Fix mount segv. • Fix mount segv's.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Fix unterminated string in hwclock.sh (thanks, Jones Lee). • Re-sync with Debian. • Cleanup the changelog entry in the uploaded package, to reduce panic. • Even newer upstream… sigh. • Fix copyright file. • New upstream. • Add amd64 to fdisk. • use absolute path to hwclock in scripts. • deal with unaligned partition table entries in fdisk. • The "SO WHY IS LETTING TWO PROCESSES OPEN THE SAME TTY FOR READ A *GOOD* THING" Release. • Admit that the kernel API doesn't provide what we need, and turn the code back off. Discussions will follow on how to deal with this post-sarge. • The I-HATE-LINUX-TTY-HANDLING Release • New and improved tty-in-use check, that actually works. • Fix tty-in-use check. Many thanks to Samuel Thibault for tracking this down and providing a patch. • Have pri= only affect that entry in swapon -a. • Mention the freshmeat site. • fix disk sun label creation in fdisk. • Use a more general form for uname. • Provide fdisk-udeb for sparc.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Cleanup vty code in getty. • Changes from Javier Fernandez-Sanguino Pen~a <jfs@computer.org> ○ Added amd64 architecture ○ Fixed manpage to avoid pointing to non existant files ○ Fixed Theodore Tso's address to the new one in dmesg ○ Modified cfdisk's es.po in order to not ask for an accented character since it will not be shown in cfdisk and causes confusion amongst users, this change could be reverted when upstream manages 8-bit characters better ○ mkswap manpage now mentiones --sparece=never option to cp ○ Added upstream maintainers to debian/copyright • Clean up FTBFS isses. • Deal with hwclock.sh on s390x. • Have getty check before opening a device. • Fix compile error in get_blocks.c. • Help out fdisk-udeb. • Version the build-depends on slang1-utf8-dev to make life clearer for woody backporters… • Deliver pg. • Re-add support for kerneli (if cryptoapi is there, we use it. If not, we assume that -e <name> refers to kerneli). • release to unstable.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Fix package priorities. • Cleanup cryptoapi patch. (Really just needed the keybits patch.) • New upstream release. • cryptoapi patch (sort of) migrated forward, along with code inspired by the patch in #206396. Still fighting with 2.4.22 crypto api, patches welcome. • Fix mount -p (to make -p an accepted option), and add back in okeybits= to make the natives happy. • Merge in dependency change from -4.1, and cleanup the dirty diff that brought. • Was creating invalid swap files. • Fix LSB failures in cal. • Fix wall copyright, patch from Shaul Karl. • Fix HURD patch. • Include cramfs support. • Fix configure bug. • Create /etc/mtab mode 0600. • Fix man page ref to rpc.nfsd(8). • Non-maintainer upload. • Correct build-depend from slang1-dev to slang1-utf8-dev to get cfdisk in fdisk-udeb to link with the same slang library as the other d-i modules. Patch from Joe Nahmias. • Put ddate back in, just to keep the natives quiet. • Fix bashism in postinst from hurd port.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Drop ddate. • Clean up messages in hwclock.sh. • Some package description changes. • properly install changelog. • Fix hwclock man page reference to /usr/local/timezone. • add in hurd patch. • Actually fixed in 2.11z-1 (or earlier)… • Install line. • Suggest dosfstools (home of mkfs.vfat). • New upstream version. • Fix sparc build. sigh. • New upstream version • don’t build fdisk on m68k. • Honor HWCLOCKACCESS in hwcolockfirst.sh. • New upstream version. • Include errno.h where needed. • Fix changelog. • New upstream release • Incorporate udeb fix from Tollef Fog Heen. • Build fdisk-udeb only where we built fdisk… • NMU with maintainer’s permission	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Generate udeb with *fdisk in it. • New maintainer. • Fix Standards-Version. • Loosen dependency of util-linux-locales to match upstream version. • Orphaned this package. • Applied a patch to hwclock/cmos.c that should fix the compilation on alpha. • New upstream release. ○ It’s now possible to build pivot_root on all architectures. ○ The confusing error message in mount is fixed. ○ minix v2 filesystems are now autodetected by mount. ○ tmpfs is now documented in mount (8). ○ s/top/Top/g in ipc.texi. • New upstream release. The following bugs are fixed in this release: ○ "setterm -foreground default" does work now. ○ "more" on empty files does no longer print junk on powerpc. ○ The entry in the expert menu the option to create a SGI disklabel is now called "create an IRIX (SGI) partition table". • debian/rules: "raw" does now compile on m68k. • Remove the special handling for PowerPC/PReP machines from the postinst.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Corrected the bug introduced in the last upload that did let the installation of util-linux fail on powerpc. • s/"uname -m"/uname -m/ in the postinst of util-linux. • Don’t install debian/tmp/DEBIAN/conffiles on s390 (since there’s no longer a hwclock on s390). • Don’t install hwclock on s390. • Make the warning in hwclockfirst.sh that occurs when the timezone couldn’t be determined more silent. • New upstream release that consists of bug fixes and several security fixes. ○ renice does no longer incorrectly report a priority of 20. ○ Upstream has included the "replay" script written by Joey Hess <joeyh@debian.org>. • Added a hwclockfirst.sh script that runs before S20modutils. • New upstream release. ○ This release contains some fixes in more (1). • Don’t build pivot_root on ia64 (ia64 has broken kernel headers). • m68k doesn’t has pivot_root, too. • Don’t build "raw" on m68k because it doesn’t compile. • hwclock.sh does now check $HWCLOCKACCESS. • New upstream release. • fdisk does now know about the partition type of the Linux/PA-RISC boot loader. • New upstream release. Bugs fixed in this release:	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ Fix for big endian architectures in disk-utils/raw.c. ○ Support for SuperH in mount. ○ The alpha options in hwclock do now work as documented. ○ mount (8) does now mention that the quota utilities do use the *quota options in /etc/fstab. • New upstream release. This release contains fixes for the following bugs: ○ Different fix for the problems with the "user" option in umount. ○ Support x86 RTC on UltraSPARC III’s. ○ An error message in mount is now proper english. • Install more.help in /usr/share/util-linux. • Updated README.Debian.hwclock.gz. • Corrected the "charset" in po/nl.po . • Standards-Version: 526.7.8.9.13-Foo.6 • Made util-linux-locales binary-all. • Applied a fdisk patch for hppa and added hppa to fdisk_arch in debian/rules. • Fixed the bug in umount that did let a user umount a file system mounted by root when the "user" option is set in /etc/fstab. • Corrected a build error on powerpc in debian/rules. • Corrected in util-linux-locales: Section : base → utils Priority: required → optional • Added the crypto patch again. Fixed in the new crypto patch:	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ It’s now the complete crypto patch. ○ "losetup" no longer lists the available ciphers. ○ It already includes the patch from #68804. ● Added blockdev to util-linux. ● Include pivot_root in util-linux. ● Added a lintian override for mount and umount. ● New upstream release. This release fixes the following bugs: ○ the problem with extended partitions when using the "o" command in fdisk is fixed ○ adfs options are now documentated in mount (8) ○ missing .TP in mount (8) was added ● The locales are now in a seperate util-linux-locales package that is not essential. ● util-linux "Suggests: kbd | console-tools" to help people to find where "kbdrate" is. ● Added support for devfs in rdev. ● Include the "raw" program in util-linux. ● Include fdformat again. ● Moved the "install-info" call from the postrm to the prerm. ● Install "HOSTORY" as "changelog.gz" in all packages. ● Removed the "swapdev" link to "rdev". Upstream says about swapdev: Nevertheless, all this is ancient junk. I just checked swapdev and found that it was last used in	

Date	Package	CVE(s)	Synopsys	Hardware Version
			kernel 0.12 but that swapdev (or rdev -s) has not done anything in any kernel later than 0.12. - Corrected the location of the examples in getopt (1). - Added the missing build dependency on gettext. - Added mips, mipsel and ia64 to fdisk_arch in debian/rules. - New upstream release. - This release contains a fix for an overrun sprintf in mount. - A message of cfdisk is less confusing in this release. - Don't include a group writable /usr/share/locale/da . - New upstream release. - Upstream removed "kbdrate" from util-linux (it's now in the packages kbd and console-tools). Let util-linux conflict with kbd (<< 1.05-3) and console-tools (<< 1:0.2.3-21) to avoid that a user of these packages has a system without "kbdrate". - New maintainer. - New upstream release, - login-utils/wall now checks whether the devices has a colon in it and skips it if it does. This prevents wall from trying to send to X connectiosn. - added joeyh's script patch for handling SIGWINCH, - debian has long been modifying the man page to point at proper file locations, these two bugs were merged with two other bugs that are actually bugs in docs v. reality and so were not getting closed. unmerged and are now being closed. - DEB_HOST_ARCH is set if not run from within dpkg-buildpackage,	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• devfs code now in the upstream, • upstream fixed the wrong NAME, • umount knows that mips does not support umount2, • removed calls to suidregister • orphaning package • New upstream release • New maintainer (possibly temporarily) • I left out the alpha fdisk patch and the crypto patch. Debian needs to line up with the upstream. If there is demand, will see what I can do. • has patch for autofs from #31251, • loop mounts leaking seems to have been fixed long ago, • nfs(5) updated to mention (no)lock option, • umount sigsegv'ing when user lacks permisions seems to have been fixed long ago, • FHS transition started in last upload forgot to, • umount -f is now documented and tries to be functional, • for all of those "please update this package" bugs, • umount -f seems to work now, I believe it was a kernel issue, • bsdutils description cleaned, no longer refers to missing binaries, • Patch rejected by upstream, • problems with alpha and bsd partitions believed fixed in 2.9w,	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• /dev/vcsa patch accepted, • msglevel fixed by upstream, • update-mime call seems to have been fixed in previous release, • looks like user error, • does not look valid any more, • LVM supported in current release, • forgot to • prerm typo, oops, • fdformat is just a wrapper, no more confusing messages, • hwclock.sh supports a BADYEAR argument from etc/default/rcS. • no longer include example.files, they do not readily apply to debian • New upstream release • NMU with maintainer’s permission • added Build-Depends, • upstream added the patch from #36340, so • upstream put '--More--' back to reverse video, • hwclock man page points at /usr/share/zoneinfo, not usr/lib • all created packages' postints now sets usr/doc/ symlink, its prerm removes said link	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• copyright file now points to usr/share/common-licenses and the typo in the URL was fixed (it is misc, not Misc) • update hwclock.sh to reflect FHS changes • debian/rules file brought up to date for FHS • elvtune man page put with the binary • The above changes allow • edited fr.po, fixed "Nombre de partitions" to "Numero de partition", • whereis knows that /usr/share/man/* is valid, • debian/rules now sets SHELL to bash, so it can use bashisms, • upstream HISTORY file included as changelog.gz, • removed /etc/fdprm, • made fdformat a sh script instead of a bash script (the bash was unneeded) • New upstream code. Add elvtune. • New upstream code. • Non-Maintainer Upload • Patch from Ben Collins to fix the -v[01] option in mkswap • Patch from Chris Butler to fix hwclock's handling of RTC • Change to line 879 of fdiskbsdlabel.c to allow building on sparc (patch sent to maintainer) • Patch from David Huggins-Daines <dhd@linuxcare.com> which is required to get a working fdisk on alpha.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Patch for mips support from Florian Lohoff <flo@rfc822.org>. • included patch from David Huggins-Daines <dhuggins@linuxcare.com> so that fdisk behaves correctly with OSF/1 disklabels. • (Important bug) * Now that 2.10f-1 has been tested in unstable, re-upload it to frozen. • New upstream release: • Security fix for mount (okir) • Avoid infinite loop in namei (Brett Wuth) • added clock-ppc.c (from Matsuura Takanori), not merged yet • deleted clockB subdirectory • recognize mkdosfs string (Michal Svec) • New: rename • Added option to mkswap so that user can override pagesize • fdisk -l now reads /proc/partitions when no device was given • Fixed fdisk.8 (James Manning) • Added devpts info to mount.8 (Elrond) • Newline fix for logger output to stdout (Henri Spencer) • There is no real concensus about what we should do about the hwclock issue. Now at least the problem is enough documented to let the user decide. (Thanks to Henrique M Holschuh <hmh+debianml@rcm.org.br> for the patch). When this package is installed, I'll examine one by one which BR can be closed. • kbdrate isn't suid anymore.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			● Included patch from "J.H.M. Dassen (Ray)" <jhm@cistron.nl>: ○ Restored enhanced losetup(8) manpage. ○ Restored encrypted filesystem support, by applying util-linux-2.9w from patch-int-2.2.13.3.gz as found on ftp.kerneli.org (modified to work with Debian's kernel-patch-int's crypto.h). ● Recompiled with ncurses5. ● ipcrm now accepts multiple ids thanks to a patch from Topi Miettinen. ● fix postinst script: ● Disabled 'hwclock --adjust' on boot. ● cfdisk must be build with slang; not ncurses. ● New upstream release. ● Put renice manpage in section 1 instead of 8. ● kbdrate's PAM now uses pam_unix.so by default. ● already fixed in 2.10-5: ● Patch by Topi Miettinen <Topi.Miettinen@nic.fi> to a longstanding bug in logger. ● replace fdformat by a notice asking to use superformat instead. ● remove setfdprm; ● conflict/replace with fdisk on sparc. ● re-introduce missing c?fdisk... (oops ;) ● Do TheRightThing(tm) for bug #47219.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• from NMU prepared by Torsten Landschoff <torsten@debian.org>: • Fixed case expression in hwclock.sh • Added usage information to hwclock • Upstream has long changed mount.c to handle nouser properly • Excluded clock.8 link from powerpc build • Replaced "$(shell dpkg --print-architecture)" with "$DEB_HOST_ARCH" in debian/rules. • New upstream release. • make /etc/rc{0,6}.d/*hwclock.sh correctly. • Correct kdbrate pam entry. • Fix fdiskdsblabel.h. • Use jgg’s patch for hwclock.sh • Really link kbdrate with pam. • New upstream release. • Include PowerPC patch from Matt Porter <mporter@phx.mcd.mot.com>. • Should be 100% PAMified(tm). Please report anomalies. • updated losetup.8 from "J.H.M. Dassen (Ray)" <jdassen@wi.LeidenUniv.nl>. • Upstream upgrade: util-linux 2.9w: • Updated mount.8 (Yann Droneaud) • Improved makefiles	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Fixed flaw in fdisk util-linux 2.9v: • cfdisk no longer believes the kernel’s HDGETGEO (and may be able to partition a 2 TB disk) util-linux 2.9u: • Czech more.help and messages (Jii Pavlovsky) • Japanese messages (Daisuke Yamashita) • fdisk fix (Klaus G. Wagner) • mount fix (Hirokazu Takahashi) • agetty: enable hardware flow control (Thorsten Kranzkowski) • minor cfdisk improvements • fdisk no longer accepts a default device • Makefile fix • now uses the script(1) supplied with util-linux instead of the one from the old bsdutils package. • remove alpha specific build patch: • remove useless warning in preinst. • include missing fdformat, setfdprm. (How comes nobody noticed yet?!) • recompile against slang1-dev 1.2.2-3. • correct hwclock.sh; • Non-maintainer upload. • Applied util-linux-2.9s.patch from patch-int-2.2.10.4.gz as found on ftp.kerneli.org to enable support for mounting encrypted filesystems through the loopback devices when using an international kernel. (Fixes: Bug#36939, #38371)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Include <linux/loop.h> and <linux/crypto.h> in the source, so as not to rely on source outside main. • Updated the losetup(8) manpage. • Upstream upgrade: • national language support for hwclock • Japanese messages (both by Daisuke Yamashita) • German messages and some misc i18n fixes (Elrond) • Czech messages (Jii Pavlovsky) • wall fixed for /dev/pts/xx ttys • make last and wall use getutent() (Sascha Schumann) [Maybe this is bad: last reading all of wtmp may be too slow. Revert in case people complain.] • documented UUID= and LABEL= in fstab.5 • added some partition types • swapon: warn only if verbose • changed hwclock.sh to get rid of a lintian error. • Added missing *.gmo files • Re-add Harmut’s powerpc patch that somehow got left out • Fix stupid bug #37916. • Upstream upgrade. • Now compiled with PAM=yes. • initial .it localisation. • Improved .fr translation.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• corrected hwclock.sh (reassigned #35429 back to sysvinit). • put rev into /usr/bin instead of /usr/sbin (Fix #34188,#35421). • include getopt examples (Fix #34705). • Upstream upgrade. • This source package now also provides the 'bsdutils' binary package. • Included patch for logger.1 from and1000@debian.org. • Included patch to logger.c from Joey • renice.c: include <errno.h> • re-use script(1) from the 'old' bsdutils package as well as README.script • Now umount is compiled with '-f' support • Re-add suidregister support for mount • modify mount.8 manpage to warn that nosuid is useless if something like suidperl is installed. (doesn't fix the critical bug #31980 reported on suidperl, but at least warn about its existance) • add missing manpages (ramsize,rootflags,swapdev) • #32414: changed a 'rm' into 'rm -f' so the source package builds cleanly. • also target the upload for frozen since this is the only missing package to be able to safely use kernels 2.2.x: To the FTP/Release maintainers: util-linux_2.9g has been introduced in unstable on Dec, 31st 98; so far I received no bug reports about it except for the missing manpages. Also compared to the 2.7.1 version from frozen, this package fixes *57* bugs. (see www.debian.org/Bugs/db/pa/lutil-linux.html) • Fix bug #31981.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Localised cfdisk + provided initial French translation. New translations welcome; you can get the potfile at http://www.ldsol.com/~vincent/util-linux.pot • Add rev and readprofile commands. • Updated fstab.5 regarding spaces in mount points names. • Fix bugs #32235,#31997 (missing hwclock.8 manpage). • Fix bug #32097 (missing mkswap.8 manpage). • Improve somewhat cfdisk regarding exit codes thanks to Enrique's patch (#31607). • Include patch from Hartmut Koptein for better powerpc support. • Patch from Topi Miettinen (Thanks Topi ;) to fix bug #31554,#31573. • Adopting the package from Guy Maor. • Re-add hwclock & kbdrate which had been lost (Fix bug #31476). • YA NMU. • Split mount out into separate package so as not to force the dangerous replacement of an essential package. • NMU (Part II): Fix more problems in 'mount'. • swapon now warn if swap device has insecure mode; Patch from Topi Miettinen <tom@medialab.sonera.net> (Fix bug #23249). • mount can now handle multiple hostnames for NFS mounts in fstab (Fix bug #29309). • Do'h; add missing /sbin/swapoff ;). • NMU.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• This package now provides /bin/mount & co. and thus obsoletes the mount package. • provides the ddate command (Fix bugs #30015 & #19820). • Move wtmp lockfile from /etc to /var/lock (Fix bug #29128). • Set bug #28885 to 'fixed' (this-is-not-a-bug,-but-a-feature(tm)). • Set bug #27931 to 'fixed' (works again since version 2.8). • Set bug #27723 to 'fixed' (been fixed by the ARM NMU). • Set bug #25831 to 'fixed' (hwclock now works as advertised). • Set buffering off on the output channel in chkdupexe.pl (Fix bug #22839). • Include patch for powerpc build by Joel Klecker <jk@espy.org> (Fix bug #21374). • Removed the confusing references to agetty (Fix bug #20668). • Check the result for the malloc()s added in the code to chown vcsa to root.sys (Fix bug #18696). • Include patch for sparc build by Eric Delaunay <delaunay@lix.polytechnique.fr> (Fix bug #17784). • Set bug #17752 to 'fixed' (Appear to work with current versions of xvt and /bin/more). • Include patch for alpha build by Christopher C Chimelis <chris@classnet.med.miami.edu> (Fix bug #17661). • Patch mkfs.minix doesn’t go into infinate loop any more depending on the argument passed to -i (Fix bug #17648). • Set bug #17483 to 'fixed' (now that util-linux is compiled with libc6 > =2.0.6 it should be fixed).	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Set bug #26625 to 'fixed' (this patch has already been applied). • Applied patch from Bcwhite to get mime support (Fix bug #26715). • Applied patch from Topi Miettinen <tom@medialab.sonera.net>: POSIX etc fixes: ○ ioctl(.., TCSETSF,..) → tcsetattr() ○ ioctl(.., TCGETS,..) → tcgetattr() ○ ioctl(.., TIOCGPGRP,..) → tcgetpgprp() ○ gcc -Wall warning fixes ○ write(2, ..) → write(fileno(stderr), ..) ○ vi → sensible-editor ○ added setlocale(LC_ALL, "") ○ use perror, isdigit, isprint, iscntrl where applicable ○ execv → execvp ○ added simple ELF detection OpenBSD fixes: ○ UCB fix ○ POSIX: rindex → strrchr ○ obsolete fseek flag L_SET → SEEK_SET ○ control-F == f ○ $EDITOR support (Fix bug #27635). • Link clock.8.gz to hwclock.8.gz (Fix bug #25852). • Non-maintainer upload.	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Recompiled with slang1. • Non-maintainer upload • Include /etc/init.d/hwclock.sh • Fix some of the (pre|post)(inst|rm) script wrt $1 processing Fixes: #18007: sysvinit: hwclock.sh uses GMT env variable - but how? #26904: hwclock.sh doesn’t "test -x" #24649: [Peter Kundrat <kundrat@gic.sk>] hwclock startup script #20728: util-linux: hwlock: GMT status lost? #19248: util-linux should install /etc/init.d/hwclock.sh • NMU: Added ARM architecture in 'disk-utils/fdiskbsdlabel.h' and 'disk-utils/fdiskbsdlabel.c'. • Removed '-m3' flag from arm-specific optimizations in MCONFIG. • Non-maintainer upload - new 2GB swap areas, removed hostid • upstream uses fixed more.c (line 813 had *p++) • Non-maintainer upload • recompiled with slang1 and ncurses4 • Another m68k patch from Roman Hodek <rnhodek@faui22c.informatik.uni-erlangen.de> • fdisk patch from Russell Coker <rjc@snoopy.virtual.net.au> for better behavior on IDE CD’s when HDIO_GETGEO fails. • fix getopt(1) typo. (16227) • Use slang for cfdisk. • fdisk -l tries eda also (13841). • Fix fdisk -l segfaults (15236,15603). • Install rdev on only i386 (15228).	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Don’t strip perl script (15480). • Add type 17=Hidden IFS to cfdisk (16843). • Removed sync (13291). • Added m68k hwclock patches from Roman Hodek (9870). • agetty.c: set vcs,vcsa to root.sys 600 when starting. • libc6 compile of new upstream version (10098, 11744, 13123). • Updated cfdisk to cfdisk 0.8k • Added old patches; I’ll send them upstream. • fdisk - extended paritions, exit on EOF. • mkfs - fix search paths. • mkfs.minix - set owner of root dir to invoker. • chkdupexe - remove upstream brokenness by checking PATH too. • mcookie - fix man page • whereis - fix search paths, find .gz files. • sync - put it back (doh!) • Folded in getty: • glibc patch (8815, 11687, 12738). • Set tty to 660 root.dialout (8960). • Register pager alternative (12475). • Updated cfdisk to ftp.win.tue.nl:/pub/linux/util/cfdisk-0.8i.tar.gz	

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Updated cfdisk to ftp.win.tue.nl:/pub/linux/util/cfdisk-0.8g.tar.gz (#9146) • -i from 2.5-9 removed as no longer needed. • cfdisk: really fixed cast this time so should be able to deal with >2GB disks(#6747, #8041) • fdisk, cfdisk: Added partition id 0xa6 = OpenBSD (#7571) • setterm: use putp to output (#7852) • Removed miscutils removal trick as it no longer works (#5757, #6862) • mkfs.minix: added patch from Volker Leiendecker <volker@fsing.uni-sb.de> to set owner of root directory to invoker (like mkfs.ext2). (#6902) • Fix dpkg-shlibddeps rules line for m68k (#5818) • Add undocumented "-i" flag to ignore bad partition tables when starting instead of throwing a fatal error. Let's pass this to the upstream maintainer, please. • disk-utils/cfdisk.c: cast sector number to ext2_loff_t in calls to ext2_llseek() • sys-utils/clock.c: fixed bug on machines without RTC enabled. • sys-utils/whereis.c: better path, compare function. • Install whereis, cytune, setsid. • sys-utils/clock.c: Fixed bugs when real-time clock device is enabled in kernel. • New source format. • disk-utils/fdisk.c: Added type a7 = NEXTSTEP (fixes bug 3259)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			- fdisk.c,cfdisk.c: Applied patch from Miquel van Smoorenburg <miquels@Q.cistron.nl> to let fdisk and cfdisk support Linux extended partitions. - Applied patch from Frank Neumann <Frank.Neumann@Informatik.Uni-Oldenburg.DE> for Linux/m68k support. - Install mkcookie. - disk-utils/mkfs.minix: fixed bug 3777 re parsing oddities. - misc-utils/setterm.c (tc_entry): Applied patch from Michael Nonweiler <mrn20@hermes.cam.ac.uk> to make it work with ncurses. - misc-utils/chkdupexe.pl: Fixed some bugs with duplicate path and symbolic links. Put in a better value for exedirs. - Install chkdupexe, setterm. - text-utils/more.c (getline): more now handles files with lines ending with "\r\n". Fixes Bug #2579. - Added 'priority: required' - disk-utils/fdisk.c (read_line): EOF now exits instead of looping forever. Fixes Bug #1206. - Added 'section: base' - Initial release	
2024-08-28	libtommath0	CVE-2023-36328	- Non-maintainer upload by the Debian ELTS team. - CVE-2023-36328: Prevent a series of integer overflow vulnerabilties that could have led attackers to execute arbitrary code and/or cause a denial of service (DoS). - Continuous integration changes: - Add a debian/.gitlab-ci.yml.	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
			- Add blhc failures in CI workflow.	
2024-09-29	libexpat1	CVE-2024-45490 CVE-2024-45491 CVE-2024-45492 CVE-2023-52425	- Non-maintainer upload by the ELTS Team. - Fix CVE-2024-45490: xmlparse.c does not reject a negative length for XML_ParseBuffer(), which may cause memory corruption or code execution. - Fix CVE-2024-45491: Integer overflow for nDefaultAtts on 32-bit platforms. - Fix CVE-2024-45492: Integer overflow for m_groupSize on 32-bit platforms. - Backport NULL checks from upstream version 2.2.1. - Non-maintainer upload by the ELTS Team. - Enable test-suite in d/rules. - Backporting patch for CVE-2023-52425 - DoS (resource consumption) parsing really big tokens due to O(n^2) complexity.	M400 S1600E M410 R100E S100 R100NA
2024-10-06	libgtk2.0-common	CVE-2024-6655	- Non-maintainer upload by the ELTS Team. - CVE-2024-6655: Stop looking for modules in the current directory	M400 S1600E M410 R100E S100 R100NA
2024-10-06	libgtk2.0-0	CVE-2024-6655	- Non-maintainer upload by the ELTS Team. - CVE-2024-6655: Stop looking for modules in the current directory	M400 S1600E M410 R100E S100 R100NA
2024-10-24	perl-modules	CVE-2020-16156 CVE-2023-31484	- Non-maintainer upload by ELTS team - Fix CVE-2020-16156: An attacker can prepend checksums for modified packages to the beginning of CHECKSUMS files, before the cleartext PGP headers. This makes the Module::Signature::_verify() checks in both cpan and cpanm pass. Without the sigtext and plaintext arguments to _verify(), the _compare() check	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
			is bypassed. This results in _verify() only checking that valid signed cleartext is present somewhere in the file. - Fix CVE-2023-31484: CPAN.pm does not verify TLS certificates when downloading distributions over HTTPS. - Fix follow up failure in testsuite.	
2024-10-24	perl-base	CVE-2020-16156 CVE-2023-31484	- Non-maintainer upload by ELTS team - Fix CVE-2020-16156: An attacker can prepend checksums for modified packages to the beginning of CHECKSUMS files, before the cleartext PGP headers. This makes the Module::Signature::_verify() checks in both cpan and cpanm pass. Without the sigtext and plaintext arguments to _verify(), the _compare() check is bypassed. This results in _verify() only checking that valid signed cleartext is present somewhere in the file. - Fix CVE-2023-31484: CPAN.pm does not verify TLS certificates when downloading distributions over HTTPS. - Fix follow up failure in testsuite.	M400 S1600E M410 R100E S100 R100NA
2024-11-21	libglib2.0-data	CVE-2024-52533 CVE-2024-34397	- Non-maintainer upload by the ELTS Team. - CVE-2024-52533: SOCKS4a proxy buffer overflow - Non-maintainer upload the ELTS team. - Fix CVE-2024-34397: Alicia Boya Garcia reported that the GDBus signal subscriptions in the GLib library are prone to a spoofing vulnerability. A local attacker can take advantage of this flaw to cause a GDBus-based client to behave incorrectly, with an application-dependent impact.	M400 S1600E M410 R100E S100 R100NA
2024-11-21	libglib2.0-0	CVE-2024-52533 CVE-2024-34397	- Non-maintainer upload by the ELTS Team. - CVE-2024-52533: SOCKS4a proxy buffer overflow - Non-maintainer upload the ELTS team.	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
			• Fix CVE-2024-34397: Alicia Boya Garcia reported that the GDBus signal subscriptions in the GLib library are prone to a spoofing vulnerability. A local attacker can take advantage of this flaw to cause a GDBus-based client to behave incorrectly, with an application-dependent impact.	
2024-11-28	libssl1.0.0	CVE-2023-5678 CVE-2024-0727	• Non-maintainer upload by the ELTS Team. • Backport upstream fixes for ○ CVE-2023-5678 (denial of service w/ excessively long X9.42 DH keys) ○ CVE-2024-0727 (denial of service on null field in PKCS12 file)	M400 S1600E M410 R100E S100 R100NA
2024-11-28	openssl	CVE-2023-5678 CVE-2024-0727	• Non-maintainer upload by the ELTS Team. • Backport upstream fixes for ○ CVE-2023-5678 (denial of service w/ excessively long X9.42 DH keys) ○ CVE-2024-0727 (denial of service on null field in PKCS12 file)	M400 S1600E M410 R100E S100 R100NA
2024-12-08	libavahi-client3	CVE-2023-38469 CVE-2023-38470 CVE-2023-38471 CVE-2023-38472 CVE-2023-38473 CVE-2023-1981	• Non-maintainer upload by the ELTS Team. • CVE-2023-38469: Reachable assertion in avahi_dns_packet_append_record • CVE-2023-38470: Reachable assertion in avahi_escape_label • CVE-2023-38471: Reachable assertion in dbus_set_host_name • CVE-2023-38472: Reachable assertion in avahi_rdata_parse • CVE-2023-38473: Reachable assertion in avahi_alternative_host_name	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
			- Fixed a GetAlternativeServiceName regression introduced by the CVE-2023-1981 fix in 0.6.31-5+deb8u2.	
2024-12-08	libavahi-common3	CVE-2023-38469 CVE-2023-38470 CVE-2023-38471 CVE-2023-38472 CVE-2023-38473 CVE-2023-1981	- Non-maintainer upload by the ELTS Team. - CVE-2023-38469: Reachable assertion in avahi_dns_packet_append_record - CVE-2023-38470: Reachable assertion in avahi_escape_label - CVE-2023-38471: Reachable assertion in dbus_set_host_name - CVE-2023-38472: Reachable assertion in avahi_rdata_parse - CVE-2023-38473: Reachable assertion in avahi_alternative_host_name - Fixed a GetAlternativeServiceName regression introduced by the CVE-2023-1981 fix in 0.6.31-5+deb8u2.	M400 S1600E M410 R100E S100 R100NA
2024-12-08	libavahi-common-data	CVE-2023-38469 CVE-2023-38470 CVE-2023-38471 CVE-2023-38472 CVE-2023-38473 CVE-2023-1981	- Non-maintainer upload by the ELTS Team. - CVE-2023-38469: Reachable assertion in avahi_dns_packet_append_record - CVE-2023-38470: Reachable assertion in avahi_escape_label - CVE-2023-38471: Reachable assertion in dbus_set_host_name - CVE-2023-38472: Reachable assertion in avahi_rdata_parse - CVE-2023-38473: Reachable assertion in avahi_alternative_host_name - Fixed a GetAlternativeServiceName regression introduced by the CVE-2023-1981 fix in 0.6.31-5+deb8u2.	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
2025-01-17	rsync	CVE-2024-12087 CVE-2024-12085 CVE-2024-12086 CVE-2024-12087 CVE-2024-12088 CVE-2024-12747	• Non-maintainer upload by the ELTS Team. • fix for upstream regression of CVE-2024-12087 FLAG_GOT_DIR_FLIST collission with FLAG_HLINKED • fix use-after-free in generator • Non-maintainer upload by the ELTS Team. • CVE-2024-12085 prevent information leak off the stack • CVE-2024-12086 ○ refuse fuzzy options when fuzzy not selected ○ added secure_relative_open() ○ receiver: use secure_relative_open() for basis file ○ disallow ../ elements in relpath for secure_relative_open • CVE-2024-12087 ○ Refuse a duplicate dirlist. ○ range check dir_ndx before use • CVE-2024-12088 make --safe-links stricter • CVE-2024-12747 fixed symlink race condition in sender	M400 S1600E M410 R100E S100 R100NA
2025-01-20	libtiff5	CVE-2024-7006 CVE-2023-52356 CVE-2023-25433 CVE-2023-52356 CVE-	• Non-maintainer upload by the ELTS Team. • CVE-2024-7006: NULL pointer dereference in TIFFReadDirectory/TIFFReadCustomDirectory • Fixed a bug in the CVE-2023-52356 fix. • Added a missing part of the CVE-2023-25433 fix.	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
		2023-3576	- Non-maintainer upload by the ELTS Team. - CVE-2023-52356 A segment fault could be triggered by passing a crafted tiff file to the TIFFReadRGBATileExt() API - CVE-2023-3576 A memory leak flaw was found in Libtiff's tiffcrop utility.	
2025-02-23	krb5-locales	CVE-2024-26462 CVE-2024-26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371	- Non Maintainer upload by LTS team - Fixes CVE-2024-26462 A memory leak vulnerability was found in /krb5/src/kdc/ndr.c. - Non-maintainer upload by the ELTS Team. - CVE-2024-26458: Memory leak in xmt_rmtcallres() - CVE-2024-26461: Memory leak in gss_krb5int_make_seal_token_v3() - CVE-2024-37370: GSS wrap token Extra Count field manipulation - CVE-2024-37371: Invalid GSS memory reads with manipulated tokens	M400 S1600E M410 R100E S100 R100NA
2025-02-23	libk5crypto3	CVE-2024-26462 CVE-2024-26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371	- Non Maintainer upload by LTS team - Fixes CVE-2024-26462 A memory leak vulnerability was found in /krb5/src/kdc/ndr.c. - Non-maintainer upload by the ELTS Team. - CVE-2024-26458: Memory leak in xmt_rmtcallres() - CVE-2024-26461: Memory leak in gss_krb5int_make_seal_token_v3() - CVE-2024-37370: GSS wrap token Extra Count field manipulation	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
			• CVE-2024-37371: Invalid GSS memory reads with manipulated tokens	
2025-02-23	libgssapi-krb5-2	CVE-2024-26462 CVE-2024-26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371	• Non Maintainer upload by LTS team • Fixes CVE-2024-26462 A memory leak vulnerability was found in /krb5/src/kdc/ndr.c. • Non-maintainer upload by the ELTS Team. • CVE-2024-26458: Memory leak in xmt_rmtcallres() • CVE-2024-26461: Memory leak in gss_krb5int_make_seal_token_v3() • CVE-2024-37370: GSS wrap token Extra Count field manipulation • CVE-2024-37371: Invalid GSS memory reads with manipulated tokens	M400 S1600E M410 R100E S100 R100NA
2025-02-23	libkrb5-3	CVE-2024-26462 CVE-2024-26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371	• Non Maintainer upload by LTS team • Fixes CVE-2024-26462 A memory leak vulnerability was found in /krb5/src/kdc/ndr.c. • Non-maintainer upload by the ELTS Team. • CVE-2024-26458: Memory leak in xmt_rmtcallres() • CVE-2024-26461: Memory leak in gss_krb5int_make_seal_token_v3() • CVE-2024-37370: GSS wrap token Extra Count field manipulation • CVE-2024-37371: Invalid GSS memory reads with manipulated tokens	M400 S1600E M410 R100E S100 R100NA
2025-02-23	libkrb5support0	CVE-2024-26462 CVE-2024-	• Non Maintainer upload by LTS team	M400 S1600E M410

Date	Package	CVE(s)	Synopsys	Hardware Version
		26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371	• Fixes CVE-2024-26462 A memory leak vulnerability was found in /krb5/src/kdc/ndr.c. • Non-maintainer upload by the ELTS Team. • CVE-2024-26458: Memory leak in xmt_rmtcallres() • CVE-2024-26461: Memory leak in gss_krb5int_make_seal_token_v3() • CVE-2024-37370: GSS wrap token Extra Count field manipulation • CVE-2024-37371: Invalid GSS memory reads with manipulated tokens	R100E S100 R100NA
2025-02-27	libtasn1-6	CVE-2024-12133	• Non-maintainer upload by the ELTS Team. • Fix CVE-2024-12133: Potential DoS while parsing a certificate containing numerous SEQUENCE OF or SET OF elements.	M400 S1600E M410 R100E S100 R100NA
2025-03-11	python2.7-minimal	CVE-2023-27043 CVE-2024-6232 CVE-2024-6923 CVE-2024-7592 CVE-2024-5642 CVE-2024-5535 CVE-2024-11168 CVE-2025-0938 CVE-2024-0450	• Non-maintainer upload by the ELTS team. • Fix CVE-2023-27043: The email module of Python incorrectly parses e-mail addresses that contain a special character. The wrong portion of an RFC2822 header is identified as the value of the addr-spec. In some applications, an attacker can bypass a protection mechanism in which application access is granted only after verifying receipt of e-mail to a specific domain (e.g., only @company.example.com addresses may be used for signup). • Fix CVE-2024-6232: Regular expressions that allowed excessive backtracking during tarfile.TarFile header parsing are vulnerable to ReDoS via specifically-crafted tar archives. • Fix CVE-2024-6923: The email module didn't properly quote newlines for email headers when serializing an email message allowing for header injection when an email is serialized. • Fix CVE-2024-7592: When parsing cookies that contained backslashes for quoted characters in the cookie value, the parser would use an algorithm with	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
			quadratic complexity, resulting in excess CPU resources being used while parsing the value. • Testsuite fixes: ○ test_signal: install procps (for missing /bin/kill) • Avoid Salsa-CI timeouts: Always run the testsuite subset that buildds use. Disable PGO on Salsa-CI. • CVE-2024-5642: CPython doesn’t disallow configuring an empty list ("[]") for SSLContext.set_npn_protocols() which is an invalid value for the underlying OpenSSL API. This results in a buffer over-read when NPN is used (see CVE-2024-5535 for OpenSSL). This vulnerability is of low severity due to NPN being not widely used and specifying an empty list likely being uncommon in-practice (typically a protocol name would be configured). • CVE-2024-11168: The urllib.parse.urlsplit() and urlparse() functions improperly validated bracketed hosts ([]), allowing hosts that weren’t IPv6 or IPvFuture. This behavior was not conformant to RFC 3986 and potentially enabled SSRF if a URL is processed by more than one URL parser. • CVE-2025-0938: urllib.parse.urlsplit and urlparse accepted domain names that included square brackets which isn’t valid according to RFC 1. Square brackets are only meant to be used as delimiters for specifying IPv6 and IPvFuture hosts in URLs. This could result in differential parsing across the Python URL parser and other specification-compliant URL parsers. • Testsuite fixes: ○ test_os: conditionally disable fsync/fdatasync tests under eatmydata | ○ test_ssl, test_httplib: fix tests relying on old SSL protocol ○ test_ssl: enable and fix tests for CVE 2023-40217	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ test_cookie: backport test cases for CVE 2024-7592 • Salsa-CI fixes: ○ debian/salsa-ci.yml: rename and tidy Salsa-CI configuration ○ Depend on netbase in DEP-8 tests (for /etc/services) ○ Fix test-build-all: create stamps when generating doc • Non-maintainer upload by the ELTS Team. • CVE-2024-0450: quoted-overlap zipbomb DoS	
2025-03-11	python2.7	CVE-2023-27043 CVE-2024-6232 CVE-2024-6923 CVE-2024-7592 CVE-2024-5642 CVE-2024-5535 CVE-2024-11168 CVE-2025-0938 CVE-2024-0450	• Non-maintainer upload by the ELTS team. • Fix CVE-2023-27043: The email module of Python incorrectly parses e-mail addresses that contain a special character. The wrong portion of an RFC2822 header is identified as the value of the addr-spec. In some applications, an attacker can bypass a protection mechanism in which application access is granted only after verifying receipt of e-mail to a specific domain (e.g., only @company.example.com addresses may be used for signup). • Fix CVE-2024-6232: Regular expressions that allowed excessive backtracking during tarfile.TarFile header parsing are vulnerable to ReDoS via specifically-crafted tar archives. • Fix CVE-2024-6923: The email module didn’t properly quote newlines for email headers when serializing an email message allowing for header injection when an email is serialized. • Fix CVE-2024-7592: When parsing cookies that contained backslashes for quoted characters in the cookie value, the parser would use an algorithm with quadratic complexity, resulting in excess CPU resources being used while parsing the value. • Testsuite fixes:	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ test_signal: install procps (for missing /bin/kill) • Avoid Salsa-CI timeouts: Always run the testsuite subset that buildds use. Disable PGO on Salsa-CI. • CVE-2024-5642: CPython doesn't disallow configuring an empty list ("[]") for SSLContext.set_npn_protocols() which is an invalid value for the underlying OpenSSL API. This results in a buffer over-read when NPN is used (see CVE-2024-5535 for OpenSSL). This vulnerability is of low severity due to NPN being not widely used and specifying an empty list likely being uncommon in-practice (typically a protocol name would be configured). • CVE-2024-11168: The urllib.parse.urlsplit() and urlparse() functions improperly validated bracketed hosts ([]), allowing hosts that weren't IPv6 or IPvFuture. This behavior was not conformant to RFC 3986 and potentially enabled SSRF if a URL is processed by more than one URL parser. • CVE-2025-0938: urllib.parse.urlsplit and urlparse accepted domain names that included square brackets which isn't valid according to RFC 1. Square brackets are only meant to be used as delimiters for specifying IPv6 and IPvFuture hosts in URLs. This could result in differential parsing across the Python URL parser and other specification-compliant URL parsers. • Testsuite fixes: ○ test_os: conditionally disable fsync/fdatasync tests under eatmydata | ○ test_ssl, test_httplib: fix tests relying on old SSL protocol ○ test_ssl: enable and fix tests for CVE 2023-40217 ○ test_cookie: backport test cases for CVE 2024-7592 • Salsa-CI fixes:	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ debian/salsa-ci.yml: rename and tidy Salsa-CI configuration ○ Depend on netbase in DEP-8 tests (for /etc/services) ○ Fix test-build-all: create stamps when generating doc • Non-maintainer upload by the ELTS Team. • CVE-2024-0450: quoted-overlap zipbomb DoS	
2025-03-11	libpython2.7-minimal	CVE-2023-27043 CVE-2024-6232 CVE-2024-6923 CVE-2024-7592 CVE-2024-5642 CVE-2024-5535 CVE-2024-11168 CVE-2025-0938 CVE-2024-0450	• Non-maintainer upload by the ELTS team. • Fix CVE-2023-27043: The email module of Python incorrectly parses e-mail addresses that contain a special character. The wrong portion of an RFC2822 header is identified as the value of the addr-spec. In some applications, an attacker can bypass a protection mechanism in which application access is granted only after verifying receipt of e-mail to a specific domain (e.g., only @company.example.com addresses may be used for signup). • Fix CVE-2024-6232: Regular expressions that allowed excessive backtracking during tarfile.TarFile header parsing are vulnerable to ReDoS via specifically-crafted tar archives. • Fix CVE-2024-6923: The email module didn’t properly quote newlines for email headers when serializing an email message allowing for header injection when an email is serialized. • Fix CVE-2024-7592: When parsing cookies that contained backslashes for quoted characters in the cookie value, the parser would use an algorithm with quadratic complexity, resulting in excess CPU resources being used while parsing the value. • Testsuite fixes: ○ test_signal: install procps (for missing /bin/kill) • Avoid Salsa-CI timeouts: Always run the testsuite subset that buildds use. Disable PGO on Salsa-CI.	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
			• CVE-2024-5642: CPython doesn’t disallow configuring an empty list ("[]") for SSLContext.set_npn_protocols() which is an invalid value for the underlying OpenSSL API. This results in a buffer over-read when NPN is used (see CVE-2024-5535 for OpenSSL). This vulnerability is of low severity due to NPN being not widely used and specifying an empty list likely being uncommon in-practice (typically a protocol name would be configured). • CVE-2024-11168: The urllib.parse.urlsplit() and urlparse() functions improperly validated bracketed hosts ([]), allowing hosts that weren’t IPv6 or IPvFuture. This behavior was not conformant to RFC 3986 and potentially enabled SSRF if a URL is processed by more than one URL parser. • CVE-2025-0938: urllib.parse.urlsplit and urlparse accepted domain names that included square brackets which isn’t valid according to RFC 1. Square brackets are only meant to be used as delimiters for specifying IPv6 and IPvFuture hosts in URLs. This could result in differential parsing across the Python URL parser and other specification-compliant URL parsers. • Testsuite fixes: ○ test_os: conditionally disable fsync/fdatasync tests under eatmydata | ○ test_ssl, test_httplib: fix tests relying on old SSL protocol ○ test_ssl: enable and fix tests for CVE 2023-40217 ○ test_cookie: backport test cases for CVE 2024-7592 • Salsa-CI fixes: ○ debian/salsa-ci.yml: rename and tidy Salsa-CI configuration ○ Depend on netbase in DEP-8 tests (for /etc/services)	

Date	Package	CVE(s)	Synopsys	Hardware Version
			○ Fix test-build-all: create stamps when generating doc • Non-maintainer upload by the ELTS Team. • CVE-2024-0450: quoted-overlap zipbomb DoS	
2025-03-15	libgnutls-deb0-28	CVE-2024-12243	• Non-maintainer upload by the ELTS Team. • d/control: Ensure that the package is built with nettle2, to avoid CVE 2021-4209. gnutls28 is only vulnerable when built with nettle3. • Fix CVE-2024-12243: Potential DoS while parsing a certificate containing numerous names or name constraints.	M400 S1600E M410 R100E S100 R100NA
2025-03-15	libgnutls-openssl27	CVE-2024-12243	• Non-maintainer upload by the ELTS Team. • d/control: Ensure that the package is built with nettle2, to avoid CVE 2021-4209. gnutls28 is only vulnerable when built with nettle3. • Fix CVE-2024-12243: Potential DoS while parsing a certificate containing numerous names or name constraints.	M400 S1600E M410 R100E S100 R100NA
2025-04-14	python-jinja2	CVE-2024-56326 CVE-2024-56326 CVE-2025-27516 CVE-2025-27516 CVE-2024-22195	• Non-maintainer upload by the ELTS team. • Fix CVE-2024-56326. An oversight in how the Jinja sandboxed environment detects calls to str.format allows an attacker that controls the content of a template to execute arbitrary Python code. ○ d/p/CVE-2024-56326.patch • Fix CVE-2025-27516. An oversight in how the Jinja sandboxed environment interacts with the |attr filter allows an attacker that controls the content of a template to execute arbitrary Python code. ○ d/p/CVE-2025-27516.patch • Non-maintainer upload by the ELTS team.	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsys	Hardware Version
			- CVE-2024-22195: Fix an issue where it was possible to inject arbitrary HTML attributes into the rendered HTML via the "xmlattr" filter, potentially leading to a Cross-Site Scripting (XSS) attack. It may also have been possible to bypass attribute validation checks if they were blacklist-based.	
2025-04-15	passwd	CVE-2023-4641 CVE-2023-29383	- Non-maintainer upload by the ELTS Security Team. - CVE-2023-4641: When asking for a new password, shadow-utils asks the password twice. If the password fails on the second attempt, shadow-utils fails in cleaning the buffer used to store the first entry. This may allow an attacker with enough access to retrieve the password from the memory. - CVE-2023-29383: It is possible to inject control characters into fields provided to the SUID program chfn (change finger). Although it is not possible to exploit this directly (e.g., adding a new user fails because \n is in the block list), it is possible to misrepresent the /etc/passwd file when viewed.	M400 S1600E M410 R100E S100 R100NA
2025-04-15	login	CVE-2023-4641 CVE-2023-29383	- Non-maintainer upload by the ELTS Security Team. - CVE-2023-4641: When asking for a new password, shadow-utils asks the password twice. If the password fails on the second attempt, shadow-utils fails in cleaning the buffer used to store the first entry. This may allow an attacker with enough access to retrieve the password from the memory. - CVE-2023-29383: It is possible to inject control characters into fields provided to the SUID program chfn (change finger). Although it is not possible to exploit this directly (e.g., adding a new user fails because \n is in the block list), it is possible to misrepresent the /etc/passwd file when viewed.	M400 S1600E M410 R100E S100 R100NA
2025-04-20	wget	CVE-2024-38428	- Non-maintainer upload by the ELTS Team. - CVE-2024-38428: Mishandling of semicolons in the userinfo subcomponent of a URI	M400 S1600E M410 R100E S100 R100NA
2025-04-27	libxml2	CVE-2025-32414 CVE-	- Non-maintainer upload by the ELTS Team.	M400 S1600E M410

Date	Package	CVE(s)	Synopsys	Hardware Version
		2025-32415 CVE-2022-49043 CVE-2024-56171 CVE-2025-24928 CVE-2025-27113 CVE-2016-9318 CVE-2017-16932 CVE-2023-39615 CVE-2023-45322 CVE-2024-25062 CVE-2022-2309	• CVE-2025-32414 fix for out-of-bounds memory access in the Python API • CVE-2025-32415 fix for heap-buffer-overflow in xmlSchemaIDCFillNodeTables() • Non-maintainer upload by the ELTS Security Team. • Import upstream patches for ○ CVE-2022-49043 - Use after free ○ CVE-2024-56171 - Use after free ○ CVE-2025-24928 - Stack based buffer overflow ○ CVE-2025-27113 - NULL pointer dereference • Non-maintainer upload by the ELTS Security Team. • Backport patches from the last stretch upload: ○ CVE-2016-9318 - improve handling of context input_id ○ CVE-2017-16932 - infinite recursion in parameter entities • CVE-2023-39615 - Crash with XML_PARSE_SAX1 Parser option • CVE-2023-45322 - Use after free after memory allocation • CVE-2024-25062 - Use after free with DTD validation and XInclude expansion enabled • Non-maintainer upload by the ELTS Team. • CVE-2022-2309: Parser NULL pointer dereference	R100E S100 R100NA
2025-05-20	vim-common	CVE-2023-4738 CVE-2024-	• Non-maintainer upload by the Security Team.	M400 S1600E M410

Date	Package	CVE(s)	Synopsys	Hardware Version
		22667 CVE-2024-43802 CVE-2024-47814 CVE-2023-4752 CVE-2023-4781 CVE-2023-5344	• CVE-2023-4738: buffer-overflow in vim_regsub_both • CVE-2024-22667: stack-buffer-overflow in option callback functions • CVE-2024-43802: heap-buffer-overflow in ins_typebuf • CVE-2024-47814: use-after-free when closing a buffer • Fix arch:all build • Non-maintainer upload by the ELTS Team. • CVE-2023-4752: Heap use after free in ins_compl_get_exp() • CVE-2023-4781: Heap buffer-overflow in vim_regsub_both() • CVE-2023-5344: Heap buffer-overflow in trunc_string()	R100E S100 R100NA

Last updated 2025-05-26 01:15:58 EDT