Sensus Approved Updates

April 7, 2025

The following updates were released by Debian and included in Unified environments in March 2025. Sensus has reviewed these updates and applied them to our Base Station environments for validation. Security updates for Unified v2.8.1 and v2.9.3 are included in this report.

Please review the below updates for installation in your environment. Sensus recommends applying any changes to a Test/Quality Assurance environment before releasing to a production environment.

For additional information and updates please visit https://www.xylem.com/en-us/about-xylem/cybersecurity/sensus-product-security/

Unified v2.8.1 Security Updates

This table describes the security updates available for Unified v2.8.1 base stations since the last update, through **2025-03-31**.

Date	Package	CVE(s)	Synopsis	Hardware Version

2025-02-21	libxml2	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 CVE-2022-29824 CVE-	• 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
				M400
				M410
				R100E
				R100NA
				S1600E
				S100

Date	Package	CVE(s)	Synopsis	Hardware Version
		2022-23308	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 • 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	

Date	Package	CVE(s)	Synopsis	Hardware Version
			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	
2025-02-23	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	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			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	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	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			maliciously.	
2025-02-23	libgssapi-krb5-2	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	libkrb5-3	CVE-2024-26462 CVE-2024-26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371 CVE-2023-36054 CVE-2022-	• 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	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
		42898	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.	
2025-02-23	libkrb5support0	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	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			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.	
2025-02-27	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-2024-7592 CVE-2024-5642 CVE-2024-5535 CVE-2024-11168 CVE-2025-0938 CVE-2024-0450 CVE-2021-23336	• 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	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
		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-2021-4189 CVE-2019-16935 CVE-2021-4189 CVE-2021-3177	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	

Date	Package	CVE(s)	Synopsis	Hardware Version
			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	

Date	Package	CVE(s)	Synopsis	Hardware Version

			• 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	

Date	Package	CVE(s)	Synopsis	Hardware Version
			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	

Date	Package	CVE(s)	Synopsis	Hardware Version
			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.	

Date	Package	CVE(s)	Synopsis	Hardware Version
			• 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-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-	• 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	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
		3737 CVE-2022-45061 CVE-2021-3177 CVE-2019-16935 CVE-2021-4189 CVE-2019-16935 CVE-2021-4189 CVE-2021-3177	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	

Date	Package	CVE(s)	Synopsis	Hardware Version
			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.	

Date	Package	CVE(s)	Synopsis	Hardware Version
			• 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 • 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	

Date	Package	CVE(s)	Synopsis	Hardware Version
			(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)	

Date	Package	CVE(s)	Synopsis	Hardware Version
			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.	

Date	Package	CVE(s)	Synopsis	Hardware Version
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 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-2021-4189 CVE-2019-16935 CVE-2021-4189 CVE-2021-3177	• 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	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			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.	

Date	Package	CVE(s)	Synopsis	Hardware Version

			• 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-	

Date	Package	CVE(s)	Synopsis	Hardware Version
			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	

Date	Package	CVE(s)	Synopsis	Hardware Version
			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	

Date	Package	CVE(s)	Synopsis	Hardware Version
			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	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			Encrypt certificates starting 2021-10-01. https://lists.debian.org/debian-lts/2021/09/msg00008.html	
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. • 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

Unified v2.9.3 Security Updates

This table describes the security updates available for Unified v2.9.3 base stations since the last update, through **2025-03-31**.

Date	Package	CVE(s)	Synopsis	Hardware Version
2025-02-21	libxml2	CVE-2022-49043 CVE-2024-56171 CVE-2025-24928 CVE-2025-27113 CVE-2016-9318 CVE-2017-16932 CVE-2023-	• 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	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
		39615 CVE-2023-45322 CVE-2024-25062 CVE-2022-2309	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	
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	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
			Extra Count field manipulation • CVE-2024-37371: Invalid GSS memory reads with manipulated tokens	
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 • CVE-2024-37371: Invalid GSS memory reads with manipulated tokens	M400 S1600E M410 R100E S100 R100NA
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

Date	Package	CVE(s)	Synopsis	Hardware Version
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-2024-26458 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
2025-02-27	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	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
			or SET OF elements.	
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 quadratic complexity, resulting in excess CPU resources being used while parsing the value. • Testsuite fixes: ○ test_signal: install procps (for missing	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
			/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	

Date	Package	CVE(s)	Synopsis	Hardware Version
			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	
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-	• 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	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
		11168 CVE-2025-0938 CVE-2024-0450	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	

Date	Package	CVE(s)	Synopsis	Hardware Version
			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-	

Date	Package	CVE(s)	Synopsis	Hardware Version
			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	
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	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
			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: o 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	

Date	Package	CVE(s)	Synopsis	Hardware Version
			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	

Date	Package	CVE(s)	Synopsis	Hardware Version
			/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	
2025-03-15	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