Sensus Approved Updates

June 2, 2025

The following updates were released by Debian and included in Unified environments in May 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 **2025-05-26**.

Date	Package	CVE(s)	Synopsis	Hardware Version

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
		CVE-2022-29824
		CVE-2022-23308
			• 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
				M400
				M410
				R100E
				R100NA
				S1600E
				S100

Date	Package	CVE(s)	Synopsis	Hardware Version

			• 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
			• 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.	

Date	Package	CVE(s)	Synopsis	Hardware Version
			• 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 CVE-2024-47814 CVE-2023-4752 CVE-2023-4781	• Non-maintainer upload by the Security Team. • CVE-2023-4738: buffer-overflow in vim_regsub_both • CVE-2024-22667: stack-buffer-	M400 M410 R100E R100NA S1600E

Date	Package	CVE(s)	Synopsis	Hardware Version
		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	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() • 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,	S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			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. • 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	

Date	Package	CVE(s)	Synopsis	Hardware Version
			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.	

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 **2025-05-26**.

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

Date	Package	CVE(s)	Synopsis	Hardware Version
			○ 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	
2025-05-20	vim-common	CVE-2023-4738 CVE-2024-22667 CVE-2024-43802 CVE-2024-47814 CVE-2023-4752 CVE-2023-4781	• Non-maintainer upload by the Security Team. • CVE-2023-4738: buffer-overflow in vim_regsub_both • CVE-2024-22667: stack-buffer-	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
		CVE-2023-5344	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()	