Sensus Approved Updates

December 2, 2024

The following updates were released by Debian and included in Unified environments in November 2024. 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 **2024-11-25**.

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

Date	Package	CVE(s)	Synopsis	Hardware Version
			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.	R100NA S1600E S100

2024-11-02	libxml2	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 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
				M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			• 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	

Date	Package	CVE(s)	Synopsis	Hardware Version
			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	
2024-11-21	libglib2.0-data	CVE-2024-52533 CVE-2024-34397 CVE-2023-29499 CVE-2023-32611 CVE-2023-32665 CVE-2021-3800 CVE-2021-28153 CVE-2021-27218 CVE-2021-27219	• 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. • 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	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			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.	
2024-11-21	libglib2.0-0	CVE-2024-52533 CVE-2024-34397 CVE-2023-29499 CVE-2023-32611 CVE-2023-	• Non-maintainer upload by the ELTS Team. • CVE-2024-52533: SOCKS4a proxy buffer overflow • Non-maintainer upload the ELTS team.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
		32665 CVE-2021-3800 CVE-2021-28153 CVE-2021-27218 CVE-2021-27219	• 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	

Date	Package	CVE(s)	Synopsis	Hardware Version
			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.	

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 **2024-11-25**.

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

Date	Package	CVE(s)	Synopsis	Hardware Version
			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

2024-11-02	libxml2	CVE-2016-9318 CVE-2017-16932 CVE-2023-39615 CVE-2023-45322 CVE-2024-25062 CVE-2022-2309	• 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
				M400
				S1600E
				M410
				R100E
				S100
				R100NA

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

Date	Package	CVE(s)	Synopsis	Hardware Version
			dependent impact.	