Sensus Approved Updates

February 3, 2025

The following updates were released by Debian and included in Unified environments in January 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 **2025-01-27**.

Date	Package	CVE(s)	Synopsis	Hardware Version

2024-11-28	libssl1.0.0	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-2022-0778 CVE-2021-3712	• 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
				M400
				M410
				R100E
				R100NA
				S1600E
				S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			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 It's partially superseded by the above changes (handling of extra extensions). The other part, supporting DER files, is obsolete and removed in later releases, and has the potential of suffering from the issue we're fixing here (command injection via filenames), so be safe and drop it.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. • CVE-2022-1292: Do not use shell to invoke openssl in c_rehash. • Non-maintainer upload by the ELTS team.	

Date	Package	CVE(s)	Synopsis	Hardware Version
			• 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-2022-0778 CVE-2021-3712	• 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
				M400
				M410
				R100E
				R100NA
				S1600E
				S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			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. • CVE-2022-1292: Do not use shell to invoke openssl in c_rehash. • Non-maintainer upload by the ELTS team.	

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

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

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

Date	Package	CVE(s)	Synopsis	Hardware Version
		26720	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.	
2025-01-17	rsync	CVE-2024-12087 CVE-2024-12085 CVE-2024-12086 CVE-2024-12087	• Non-maintainer upload by the ELTS Team. • fix for upstream regression of CVE-2024-12087 FLAG_GOT_DIR_FLIST collission with FLAG_HLINKED	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version

		CVE-2024-12088 CVE-2024-12747	• 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	

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	• 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 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
		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-2022-3627 CVE-2020-19144 CVE-2020-19131	• 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	

Date	Package	CVE(s)	Synopsis	Hardware Version
			tiff file can lead to an out-of-bounds write or read resulting in a denial of service. • 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)	

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 **2025-01-27**.

Date	Package	CVE(s)	Synopsis	Hardware Version

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	M400 S1600E M410 R100E S100 R100NA

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

Date	Package	CVE(s)	Synopsis	Hardware Version
			regression introduced by the CVE-2023-1981 fix in 0.6.31-5+deb8u2.	

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	• Non-maintainer upload by the ELTS Team. • CVE-2024-7006: NULL pointer	M400 S1600E M410

Date	Package	CVE(s)	Synopsis	Hardware Version
		CVE-2023-25433 CVE-2023-52356 CVE-2023-3576	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.	R100E S100 R100NA