Sensus Approved Updates

November 4, 2024

The following updates were released by Debian and included in Unified environments in October 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 **2024-10-28**.

Date	Package	CVE(s)	Synopsis	Hardware Version
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-2022-25313 CVE-2022-25315 CVE-2022-25236 CVE-2022-23852 CVE-2021-46143 CVE-2022-22825 CVE-2022-23990	• 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	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			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	

Date	Package	CVE(s)	Synopsis	Hardware Version
			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.	
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

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 **2024-10-28**.

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

Date	Package	CVE(s)	Synopsis	Hardware Version
			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.	
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