Sensus Approved Updates

May 5, 2025

The following updates were released by Debian and included in Unified environments in April 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 **2025-04-28**.

Date	Package	CVE(s)	Synopsis	Hardware Version
2025-04-14	python-jinja2	CVE-2024-56326 CVE-2024-56326 CVE-2025-27516 CVE-2025-27516 CVE-2024-22195	• Non-maintainer upload by the ELTS team. • Fix CVE-2024-56326. An oversight in how the Jinja sandboxed environment detects calls to str.format allows an attacker that controls the content of a template to execute arbitrary Python code. ○ d/p/CVE-2024-56326.patch • Fix CVE-2025-27516. An oversight in how the Jinja sandboxed environment interacts with the |attr filter allows an attacker that controls the content of a template to execute arbitrary Python code. ○ d/p/CVE-2025-27516.patch • Non-maintainer upload by the ELTS team.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			- CVE-2024-22195: Fix an issue where it was possible to inject arbitrary HTML attributes into the rendered HTML via the "xmlattr" filter, potentially leading to a Cross-Site Scripting (XSS) attack. It may also have been possible to bypass attribute validation checks if they were blacklist-based.	
2025-04-15	passwd	CVE-2023-4641 CVE-2023-29383 CVE-2017-12424 CVE-2017-12424 CVE-2018-7169 CVE-2018-7169	- Non-maintainer upload by the ELTS Security Team. - CVE-2023-4641: When asking for a new password, shadow-utils asks the password twice. If the password fails on the second attempt, shadow-utils fails in cleaning the buffer used to store the first entry. This may allow an attacker with enough access to retrieve the password from the memory. - CVE-2023-29383: It is possible to inject control characters into fields provided to the SUID program chfn (change finger). Although it is not possible to exploit this directly (e.g., adding a new user fails because \n is in the block list), it is possible to misrepresent the /etc/passwd file when viewed. - Non-maintainer upload by the ELTS team. - SECURITY UPDATE: Crash or buffer overflow ○ debian/patches/CVE-2017-12424.patch: fix buffer overflow if NULL line is present in db in	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			lib/commonio.c. ○ CVE-2017-12424 • SECURITY UPDATE: Access to privileged information ○ debian/patches/CVE-2018-7169.patch: newgidmap: enforce setgroups=deny if self-mapping a group in src/newgidmap.c. ○ CVE-2018-7169	
2025-04-15	login	CVE-2023-4641 CVE-2023-29383 CVE-2017-12424 CVE-2017-12424 CVE-2018-7169 CVE-2018-7169	• Non-maintainer upload by the ELTS Security Team. • CVE-2023-4641: When asking for a new password, shadow-utils asks the password twice. If the password fails on the second attempt, shadow-utils fails in cleaning the buffer used to store the first entry. This may allow an attacker with enough access to retrieve the password from the memory. • CVE-2023-29383: It is possible to inject control characters into fields provided to the SUID program chfn (change finger). Although it is not possible to exploit this directly (e.g., adding a new user fails because \n is in the block list), it is possible to misrepresent the /etc/passwd file when viewed. • Non-maintainer upload by the ELTS team. • SECURITY UPDATE: Crash or buffer overflow ○ debian/patches/CVE-2017-12424.patch:	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			fix buffer overflow if NULL line is present in db in lib/commonio.c. ○ CVE-2017-12424 • SECURITY UPDATE: Access to privileged information ○ debian/patches/CVE-2018-7169.patch: newgidmap: enforce setgroups=deny if self-mapping a group in src/newgidmap.c. ○ CVE-2018-7169	
2025-04-20	wget	CVE-2024-38428	• Non-maintainer upload by the ELTS Team. • CVE-2024-38428: Mishandling of semicolons in the userinfo subcomponent of a URI	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 **2025-04-28**.

Date	Package	CVE(s)	Synopsis	Hardware Version
2025-04-14	python-jinja2	CVE-2024-56326 CVE-2024-56326 CVE-2025-27516 CVE-2025-27516 CVE-2024-22195	• Non-maintainer upload by the ELTS team. • Fix CVE-2024-56326. An oversight in how the Jinja sandboxed environment detects calls to str.format allows an attacker that controls the content of a template to execute arbitrary Python code. ○ d/p/CVE-2024-56326.patch	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
			• Fix CVE-2025-27516. An oversight in how the Jinja sandboxed environment interacts with the |attr filter allows an attacker that controls the content of a template to execute arbitrary Python code. ○ d/p/CVE-2025-27516.patch • Non-maintainer upload by the ELTS team. • CVE-2024-22195: Fix an issue where it was possible to inject arbitrary HTML attributes into the rendered HTML via the "xmlattr" filter, potentially leading to a Cross-Site Scripting (XSS) attack. It may also have been possible to bypass attribute validation checks if they were blacklist-based.	
2025-04-15	passwd	CVE-2023-4641 CVE-2023-29383	• Non-maintainer upload by the ELTS Security Team. • CVE-2023-4641: When asking for a new password, shadow-utils asks the password twice. If the password fails on the second attempt, shadow-utils fails in cleaning the buffer used to store the first entry. This may allow an attacker with enough access to retrieve the password from the memory. • CVE-2023-29383: It is possible to inject control characters into fields provided to the SUID program chfn (change finger). Although it is not possible to exploit this directly (e.g., adding a new user fails because \n is in the block list), it is	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
			possible to misrepresent the /etc/passwd file when viewed.	
2025-04-15	login	CVE-2023-4641 CVE-2023-29383	• Non-maintainer upload by the ELTS Security Team. • CVE-2023-4641: When asking for a new password, shadow-utils asks the password twice. If the password fails on the second attempt, shadow-utils fails in cleaning the buffer used to store the first entry. This may allow an attacker with enough access to retrieve the password from the memory. • CVE-2023-29383: It is possible to inject control characters into fields provided to the SUID program chfn (change finger). Although it is not possible to exploit this directly (e.g., adding a new user fails because \n is in the block list), it is possible to misrepresent the /etc/passwd file when viewed.	M400 S1600E M410 R100E S100 R100NA
2025-04-20	wget	CVE-2024-38428	• Non-maintainer upload by the ELTS Team. • CVE-2024-38428: Mishandling of semicolons in the userinfo subcomponent of a URI	M400 S1600E M410 R100E S100 R100NA