SSA-836527: Multiple Vulnerabilities in SCALANCE X-300 Switch Family Devices

Publication Date:	2022-04-12
Last Update:	2022-04-12
Current Version:	V1.0
CVSS v3.1 Base Score:	9.6

SUMMARY

Several SCALANCE X-300 switches contain multiple vulnerabilities. An unauthenticated attacker could reboot, cause denial of service conditions and potentially impact the system by other means through heap and buffer overflow vulnerabilities.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE X302-7 EEC (2x 24V) (6GK5302-7GD00-2EA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (2x 24V, coated) (6GK5302-7GD00-2GA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (2x 230V) (6GK5302-7GD00-4EA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (2x 230V, coated) (6GK5302-7GD00-4GA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (24V) (6GK5302-7GD00-1EA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (24V, coated) (6GK5302-7GD00-1GA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

SCALANCE X302-7 EEC (230V) (6GK5302-7GD00-3EA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (230V, coated) (6GK5302-7GD00-3GA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X304-2FE (6GK5304-2BD00-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X306-1LD FE (6GK5306-1BF00-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (2x 24V) (6GK5307-2FD00-2EA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (2x 24V, coated) (6GK5307-2FD00-2GA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (2x 230V) (6GK5307-2FD00-4EA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (2x 230V, coated) (6GK5307-2FD00-4GA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (24V) (6GK5307-2FD00-1EA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (24V, coated) (6GK5307-2FD00-1GA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

SCALANCE X307-2 EEC (230V) (6GK5307-2FD00-3EA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (230V, coated) (6GK5307-2FD00-3GA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-3 (6GK5307-3BL00-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-3 (6GK5307-3BL10-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-3LD (6GK5307-3BM00-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-3LD (6GK5307-3BM10-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2 (6GK5308-2FL00-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2 (6GK5308-2FL10-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LD (6GK5308-2FM00-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LD (6GK5308-2FM10-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

SCALANCE X308-2LH (6GK5308-2FN00-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH (6GK5308-2FN10-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH+ (6GK5308-2FP00-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH+ (6GK5308-2FP10-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M (6GK5308-2GG00-2AA2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M (6GK5308-2GG10-2AA2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M PoE (6GK5308-2QG00-2AA2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M PoE (6GK5308-2QG10-2AA2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M TS (6GK5308-2GG00-2CA2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M TS (6GK5308-2GG10-2CA2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

SCALANCE X310 (6GK5310-0FA00-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X310 (6GK5310-0FA10-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X310FE (6GK5310-0BA00-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X310FE (6GK5310-0BA10-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X320-1 FE (6GK5320-1BD00-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X320-1-2LD FE (6GK5320-3BF00-2AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X408-2 (6GK5408-2FD00-2AA2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 24V, ports on front) (6GK5324-4GG00-2ER2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 24V, ports on front) (6GK5324-4GG10-2ER2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 24V, ports on rear) (6GK5324-4GG00-2JR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR324-4M EEC (2x 24V, ports on rear) (6GK5324-4GG10-2JR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front) (6GK5324-4GG00-4ER2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front) (6GK5324-4GG10-4ER2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG00-4JR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG10-4JR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (24V, ports on front) (6GK5324-4GG00-1ER2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (24V, ports on front) (6GK5324-4GG10-1ER2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (24V, ports on rear) (6GK5324-4GG00-1JR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (24V, ports on rear) (6GK5324-4GG10-1JR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front) (6GK5324-4GG00-3ER2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front) (6GK5324-4GG10-3ER2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG00-3JR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG10-3JR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE (24V, ports on front) (6GK5324-4QG00-1AR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE (24V, ports on rear) (6GK5324-4QG00-1HR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE (230V, ports on front) (6GK5324-4QG00-3AR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE (230V, ports on rear) (6GK5324-4QG00-3HR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE TS (24V, ports on front) (6GK5324-4QG00-1CR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (24V, ports on front) (6GK5324-0GG00-1AR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (24V, ports on front) (6GK5324-0GG10-1AR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR324-12M (24V, ports on rear) (6GK5324-0GG00-1HR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (24V, ports on rear) (6GK5324-0GG10-1HR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (230V, ports on front) (6GK5324-0GG00-3AR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (230V, ports on front) (6GK5324-0GG10-3AR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (230V, ports on rear) (6GK5324-0GG00-3HR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (230V, ports on rear) (6GK5324-0GG10-3HR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M TS (24V) (6GK5324-0GG00-1CR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M TS (24V) (6GK5324-0GG10-1CR2): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SIPLUS NET SCALANCE X308-2 (6AG1308-2FL10-4AA3): All versions < V4.1.4	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Restrict access to the affected systems, especially to ports 22/tcp, 161/udp, and 443/tcp to trusted IP addresses only

- Disable SNMP service, if possible
- Deactivate the webserver if not required, and if deactivation is supported by the product

Product specific remediations or mitigations can be found in the section Affected Products and Solution.

Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

SCALANCE X switches are used to connect industrial components like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs).

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2022-25751

Affected devices do not properly validate the HTTP headers of incoming requests. This could allow an unauthenticated remote attacker to crash affected devices.

CVSS v3.1 Base Score	8.2
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2022-25752

The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-330: Use of Insufficiently Random Values

Vulnerability CVE-2022-25753

The handling of arguments such as IP addresses in the CLI of affected devices is prone to buffer overflows. This could allow an authenticated remote attacker to execute arbitrary code on the device.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-121: Stack-based Buffer Overflow

Vulnerability CVE-2022-25754

The integrated web server of the affected device could allow remote attackers to perform actions with the permissions of a victim user, provided the victim user has an active session and is induced to trigger the malicious request.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-352: Cross-Site Request Forgery (CSRF)

Vulnerability CVE-2022-25755

The webserver of an affected device is missing specific security headers. This could allow an remote attacker to extract confidential session information under certain circumstances.

CVSS v3.1 Base Score	2.6
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

Vulnerability CVE-2022-25756

The integrated web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link. This can be used by an attacker to trigger a malicious request on the affected device.

CVSS v3.1 Base Score	7.9
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

Vulnerability CVE-2022-26334

Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices.

CVSS v3.1 Base Score	8.2
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:H/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2022-26335

Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices.

CVSS v3.1 Base Score	9.6
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input (‘Classic Buffer Overflow’)

Vulnerability CVE-2022-26380

Affected devices do not properly validate if a certain SNMP key exists. An attacker could use this to trigger a reboot of an affected device by requesting specific SNMP information from the device.

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Michael Messner and Abian Blome from Siemens Energy for coordinated disclosure of CVE-2022-25751 - CVE-2022-25756

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2022-04-12):	Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens’ underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens’ Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.