SSA-310038: Multiple Vulnerabilities in SCALANCE X Switch Devices

Publication Date: 2022-07-12
Last Update: 2022-07-12
Current Version: V1.0
CVSS v3.1 Base Score: 9.6

SUMMARY

Several SCALANCE X 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 several affected products and recommends to update to the latest versions. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE X200-4P IRT (6GK5200-4AH00-2BA3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE X200-4P IRT (6GK5200-4AH10-2BA3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE X201-3P IRT (6GK5201-3BH00-2BA3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE X201-3P IRT (6GK5201-3BH10-2BA3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE X201-3P IRT PRO (6GK5201-3BH00-2BD2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE X201-3P IRT PRO (6GK5201-3JR10-2BA6): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE X202-2IRT (6GK5202-2BB00-2BA3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE X202-2IRT (6GK5202-2BB10-2BA3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE X202-2P IRT (6GK5202-2BH00-2BA3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE X202-2P IRT (6GK5202-2BH10-2BA3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE X202-2P IRT PRO (6GK5202-2JR00-2BA6): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE X202-2P IRT PRO (6GK5202-2JR10-2BA6): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE X204-2 (6GK5204-2BB10-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204-2FM (6GK5204-2BB11-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204-2LD (6GK5204-2BC10-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204-2LD TS (6GK5204-2BC10-2CA2): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204-2TS (6GK5204-2BB10-2CA2): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204IRT (6GK5204-0BA00-2BA3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE X204IRT (6GK5204-0BA10-2BA3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE X204IRT PRO (6GK5204-0JA00-2BA6): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE X204IRT PRO (6GK5204-0JA10-2BA6): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE X206-1 (6GK5206-1BB10-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/ See further recommendations from section Workarounds and Mitigations
SCALANCE X206-1LD (6GK5206-1BC10-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/ See further recommendations from section Workarounds and Mitigations
SCALANCE X208 (6GK5208-0BA10-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/ See further recommendations from section Workarounds and Mitigations
SCALANCE X208PRO (6GK5208-0HA10-2AA6): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/ See further recommendations from section Workarounds and Mitigations
SCALANCE X212-2 (6GK5212-2BB00-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/ See further recommendations from section Workarounds and Mitigations
SCALANCE X212-2LD (6GK5212-2BC00-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/ See further recommendations from section Workarounds and Mitigations
SCALANCE X216 (6GK5216-0BA00-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/ See further recommendations from section Workarounds and Mitigations
SCALANCE X224 (6GK5224-0BA00-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/ See further recommendations from section Workarounds and Mitigations
SCALANCE XF201-3P IRT (6GK5201-3JR00-2BA6): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XF202-2P IRT (6GK5202-2BH00-2BD2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE XF204 (6GK5204-0BA00-2AF2): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/ See further recommendations from section Workarounds and Mitigations
SCALANCE XF204-2 (6GK5204-2BC00-2AF2): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/ See further recommendations from section Workarounds and Mitigations
SCALANCE XF204-2BA IRT (6GK5204-2AA00-2BD2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XF204IRT (6GK5204-0BA00-2BF2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XF204IRT (6GK5204-0BA10-2BF2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XF206-1 (6GK5206-1BC00-2AF2): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/ See further recommendations from section Workarounds and Mitigations
SCALANCE XF208 (6GK5208-0BA00-2AF2): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/ 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 port 80/tcp and port 443/tcp to trusted IP addresses only
- 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-2022-26647

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-2022-26648

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-2022-26649

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')

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 (2022-07-12): Publication Date

TERMS OF USE