SSA-187092: Several Buffer-Overflow Vulnerabilities in Web Server of SCALANCE X-200

Publication Date: 2021-04-13
Last Update: 2021-04-13
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

Several SCALANCE X-200 switches contain buffer overflow vulnerabilities in the web server.

In the most severe case an attacker could potentially remotely execute code.

Siemens is preparing 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: All versions < 5.5.1	Update to V5.5.1 or later version https://support.industry.siemens.com/cs/us/en/view/109793952/
SCALANCE X201-3P IRT: All versions < 5.5.1	Update to V5.5.1 or later version https://support.industry.siemens.com/cs/us/en/view/109793952/
SCALANCE X201-3P IRT PRO: All versions < 5.5.1	Update to V5.5.1 or later version https://support.industry.siemens.com/cs/us/en/view/109793952/
SCALANCE X202-2 IRT: All versions < 5.5.1	Update to V5.5.1 or later version https://support.industry.siemens.com/cs/us/en/view/109793952/
SCALANCE X202-2P IRT (incl. SIPLUS NET variant): All versions < 5.5.1	Update to V5.5.1 or later version https://support.industry.siemens.com/cs/us/en/view/109793952/
SCALANCE X202-2P IRT PRO: All versions < 5.5.1	Update to V5.5.1 or later version https://support.industry.siemens.com/cs/us/en/view/109793952/
SCALANCE X204 IRT: All versions < 5.5.1	Update to V5.5.1 or later version https://support.industry.siemens.com/cs/us/en/view/109793952/
SCALANCE X204 IRT PRO: All versions < 5.5.1	Update to V5.5.1 or later version https://support.industry.siemens.com/cs/us/en/view/109793952/
SCALANCE X204-2 (incl. SIPLUS NET variant): All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X204-2FM: All versions	See recommendations from section Workarounds and Mitigations

SCALANCE X204-2LD (incl. SIPLUS NET variant): All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X204-2LD TS: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X204-2TS: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X206-1: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X206-1LD: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X208 (incl. SIPLUS NET variant): All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X208PRO: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X212-2 (incl. SIPLUS NET variant): All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X212-2LD: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X216: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X224: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XF201-3P IRT: All versions < 5.5.1	Update to V5.5.1 or later version https://support.industry.siemens.com/cs/us/en/view/109793952/
SCALANCE XF202-2P IRT: All versions < 5.5.1	Update to V5.5.1 or later version https://support.industry.siemens.com/cs/us/en/view/109793952/
SCALANCE XF204: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XF204 IRT: All versions < 5.5.1	Update to V5.5.1 or later version https://support.industry.siemens.com/cs/us/en/view/109793952/
SCALANCE XF204-2 (incl. SIPLUS NET variant): All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XF204-2BA IRT: All versions < 5.5.1	Update to V5.5.1 or later version https://support.industry.siemens.com/cs/us/en/view/109793952/

SCALANCE XF206-1: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XF208: All versions	See 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:

- Limit network traffic of web servers of SCALANCE X switches to trusted connections by firewall rules (port 443/tcp and 80/tcp).

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-2021-25668

Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2021-25669

Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-121: Stack-based 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 (2021-04-13): Publication Date

TERMS OF USE