SSA-139628: Vulnerabilities in Web Server for Scalance X Products

Publication Date: 2021-01-12
Last Update: 2021-01-12
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

Several SCALANCE X switches contain vulnerabilities in the web server of the affected devices.

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 version(s). Siemens recommends countermeasures where fixes are not currently available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE X-200 switch family (incl. SIPLUS NET variants): All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X-200IRT switch family (incl. SIPLUS NET variants): All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X-300 switch family (incl. X408 and SIPLUS NET variants): All versions < V4.1.0 only affected by CVE-2020-15800	Update to V4.1.0 or later https://support.industry.siemens.com/cs/ww/en/view/109773547/

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).

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-2020-15799

The vulnerability could allow an unauthenticated attacker to reboot the device over the network by using special urls from integrated web server of the affected products.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

Vulnerability CVE-2020-15800

The webserver of the affected devices contains a vulnerability that may lead to a heap overflow condition. An attacker could cause this condition on the webserver by sending specially crafted requests. This could stop the webserver temporarily.

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:X/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2020-25226

The web server of the affected devices contains a vulnerability that may lead to a buffer overflow condition. An attacker could cause this condition on the webserver by sending a specially crafted request. The webserver could stop and not recover anymore.

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:X/RC:C
CWE	CWE-122: Heap-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 (2021-01-12): Publication Date

TERMS OF USE