SSA-447396: Denial-of-Service in SCALANCE X-300, SCALANCE X408 and SCALANCE X414

Publication Date:	2018-09-11
Last Update:	2020-02-10
Current Version:	V1.1
CVSS v3.1 Base Score:	8.6

SUMMARY

A vulnerability has been identified in the integrated web server of SCALANCE X300, SCALANCE X408, and SCALANCE X414. The vulnerability could allow an attacker with network access to the device to cause a Denial-of-Service condition.

The vulnerability can be triggered with publicly available tools, including vulnerability scanners.

Siemens provides updates for SCALANCE X300, and SCALANCE X408, and provides mitigations for the SCALANCE X414.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE X-300 switch family (incl. SIPLUS NET variants): All versions < V4.0.0	Update to V4.1.2 https://support.industry.siemens.com/cs/us/en/view/109753720
SCALANCE X408: All versions < V4.0.0	Update to V4.1.2 https://support.industry.siemens.com/cs/us/en/view/109753720
SCALANCE X414: 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:

- Protect network access to the integrated web server on port 443/tcp with appropriate mechanisms:

  Restrict network access to port 443/tcp to trusted IP addresses, and avoid running vulnerability scanning tools from trusted IP addresses on affected devices.

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-2018-13807

The web interface on port 443/tcp could allow an attacker to cause a Denial-of-Service condition by sending specially crafted packets to the web server. The device will automatically reboot, impacting network availability for other devices.

An attacker must have network access to port 443/tcp to exploit the vulnerability. Neither valid credentials nor interaction by a legitimate user is required to exploit the vulnerability. There is no confidentiality or integrity impact, only availability is temporarily impacted.

This vulnerability could be triggered by publicly available tools.

CVSS v3.1 Base Score	8.6
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:F/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

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 (2018-09-11):	Publication Date
V1.1 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products

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.