SSA-321046: Denial-of-Service Vulnerability in SCALANCE X-300/X408 Switch Family

Publication Date: 2015-01-19
Last Update: 2020-02-10
Current Version: V1.1
CVSS v3.1 Base Score: 7.5

SUMMARY

The latest firmware update for the Siemens SCALANCE X-300 switch family and SCALANCE X 408 fixes two vulnerabilities. The vulnerabilities could allow attackers to cause a device reboot under certain conditions. An attacker must have network access to the device to exploit this vulnerability.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE X-300 switch family (incl. SIPLUS NET variants): All versions < V4.0	Update to V4.0 http://support.automation.siemens.com/WW/view/en/107178573
SCALANCE X408: All versions < V4.0	Update to V4.0 http://support.automation.siemens.com/WW/view/en/107178573

WORKAROUNDS AND MITIGATIONS

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

- Siemens recommends protecting network access to all products except for perimeter devices with appropriate mechanisms
- It is advised to follow recommended security practices (see http://ics-cert.us-cert.gov/content/recommended-practices)

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-2014-8478

The web server of the affected switches could allow unauthenticated users to cause a device reboot if malformed HTTP requests are sent to the web server (port 80/tcp or port 443/tcp). To achieve this, an attacker must be able to reach the HTTP interface over the network. No packets are forwarded to connected devices until the reboot is completed.

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-20: Improper Input Validation

Vulnerability CVE-2014-8479

The FTP server of the affected switches could allow authenticated users to cause a device reboot if specially crafted network packets are sent to the FTP server (port 21/tcp). No packets are forwarded to connected devices until the reboot is completed.

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-20: Improper Input Validation

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Deja vu Security for coordinated disclosure
- 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 (2015-01-19): Publication Date
V1.1 (2020-02-10): SIPLUS devices now explicitly mentioned in the list of affected products

TERMS OF USE