SSA-130874: Multiple Security Vulnerabilities in SCALANCE X Switches

Publication Date: 2012-04-05
Last Update: 2020-02-10
Current Version: V1.3
CVSS v3.1 Base Score: 6.8

SUMMARY

A denial of service vulnerability was found in several Siemens Scalance X switches. Siemens addresses the vulnerability by two firmware upgrades.

The web server of the vulnerable switches is susceptible to a remote denial of service attack. If the attack is executed, it causes a reboot of the device and no data can be transferred over the device.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE X-300 switch family (incl. SIPLUS NET variants): All versions < V3.7.2	Update to V3.7.2 http://support.automation.siemens.com/WW/view/de/59868786
SCALANCE X414-3E: All versions < V3.7.1	Update to V3.7.1 http://support.automation.siemens.com/WW/view/de/59613294

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any specific mitigations or workarounds.

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 SVE-2012-0002

The web server of the affected switches does not sanitize URLs in HTTP requests properly. If an attacker requests a malformed URL from the web server, a vulnerable switch reboots. To achieve this, the attacker must be able to reach the administrative interface over the network.

If the attack is executed, it causes a reboot of the device and no data can be transferred over the device.

CVSS v3.1 Base Score	6.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/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:

- Jürgen Bilberger from Daimler TSS GmbH 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

V1.2 (2012-04-05): Publication Date
V1.3 (2020-02-10): SIPLUS devices now explicitly mentioned in the list of affected products

TERMS OF USE