SSA-850708: Authentication Bypass in SCALANCE X-200 Switch Family

Publication Date: 2013-09-11
Last Update: 2020-02-10
Current Version: V1.2
CVSS v3.1 Base Score: 7.6

SUMMARY

A potential vulnerability was discovered in the web server's authentication of SCALANCE X-200 switches that might allow attackers to hijack web sessions over the network without authentication. Siemens addresses the issue with a firmware update.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE X-200 switch family (incl. SIPLUS NET variants): All versions < V5.0.1	Update to firmware > V5.0.1 https://support.industry.siemens.com/cs/search?search=scalance%20x-200&type=Download&lc=en-DE

WORKAROUNDS AND MITIGATIONS

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

- Operate the device only within trusted networks.

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-2013-5709

The authentication of the integrated web server of SCALANCE X-200 switches might allow attackers to hijack web sessions over the network without authentication due to insufficient entropy in its random number generator.

CVSS v3.1 Base Score	7.6
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C
CWE	CWE-952: SFP Secondary Cluster: Missing Authentication

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Eireann Leverett from IOActive 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 (2013-09-11):	Publication Date
V1.1 (2013-10-18):	Changed recommended firmware version to V5.0.1 due to configuration issues of V5.0.0
V1.2 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products. Updated firmware download links

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.