SSA-480829: Cross-Site Scripting Vulnerabilities in SCALANCE X Switches

Publication Date: 2018-06-12
Last Update: 2022-12-13
Current Version: V1.2
CVSS v3.1 Base Score: 5.8

SUMMARY

Two cross-site scripting (XSS) vulnerabilities were identified in the web server of several SCALANCE X switches.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE X-200 switch family (incl. SIPLUS NET variants): All versions < V5.2.3 only affected by CVE-2018-4848	Update to V5.2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109758142/ See further recommendations from section Workarounds and Mitigations
SCALANCE X-200IRT switch family (incl. SIPLUS NET variants): All versions < V5.4.1	Update to V5.4.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109758144/ See further recommendations from section Workarounds and Mitigations
SCALANCE X-200RNA switch family: All versions < V3.2.7	Update to V3.2.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109814809/ See further recommendations from section Workarounds and Mitigations
SCALANCE X-300 switch family (incl. X408 and SIPLUS NET variants): All versions < V4.1.3	Update to V4.1.3 or later version https://support.industry.siemens.com/cs/document/109773547/ See further 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:

- To exploit CVE-2018-4842, the attacker needs to be able to log into the administrative web application.
- To exploit CVE-2018-4848 the attacker must trick the user to click on a link while being logged in.

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

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-2018-4842

A remote, authenticated attacker with access to the configuration web server could be able to store script code on the web site, if the HRP redundancy option is set. This code could be executed in the web browser of victims visiting this web site (XSS), affecting its confidentiality, integrity and availability.

User interaction is required for successful exploitation, as the user needs to visit the manipulated web site. At the stage of publishing this security advisory no public exploitation is known. The vendor has confirmed the vulnerability and provides mitigations to resolve it.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2018-4848

The integrated configuration web server of the affected devices could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link.

User interaction is required for a successful exploitation. The user must be logged into the web interface in order for the exploitation to succeed. At the stage of publishing this security advisory no public exploitation is known. The vendor has confirmed the vulnerability and provides mitigations to resolve it.

CVSS v3.1 Base Score	5.8
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Marius Rothenbücher for coordinated disclosure of CVE-2018-4842
- Ali Abbasi for coordinated disclosure of CVE-2018-4848
- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned
- KraftCERT for coordination efforts

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 (2018-06-12):	Publication Date
V1.1 (2020-01-14):	SIPLUS devices now explicitly mentioned in the list of affected products; added update information for SCALANCE X-300/X408
V1.2 (2022-12-13):	Added SCALANCE X-200RNA switch family

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.