SSA-951513: Clickjacking Vulnerability in SCALANCE S, SCALANCE X-300, X-200IRT, X-200RNA and X-200 Switch Families

Publication Date: 2020-02-11
Last Update: 2022-12-13
Current Version: V1.3
CVSS v3.1 Base Score: 4.2

SUMMARY

Several SCALANCE X switches contain a vulnerability that could allow an attacker to perform administrative actions if the victim is tricked into clicking on a website controlled by the attacker. The attack only works if the victim has an authenticated session on the administrative interface of the switch.

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 S602: All versions < V4.1	Update to V4.1 or later version Update is only available via Siemens Support contact Upgrade hardware to successor product from SCALANCE SC-600 family (https://support.industry.siemens.com/cs/document/109756957) and apply patches when available, or follow recommendations from section Workarounds and Mitigations See further recommendations from section Workarounds and Mitigations
SCALANCE S612: All versions < V4.1	Update to V4.1 or later version Update is only available via Siemens Support contact Upgrade hardware to successor product from SCALANCE SC-600 family (https://support.industry.siemens.com/cs/document/109756957) and apply patches when available, or follow recommendations from section Workarounds and Mitigations See further recommendations from section Workarounds and Mitigations
SCALANCE S623: All versions < V4.1	Update to V4.1 or later version Update is only available via Siemens Support contact Upgrade hardware to successor product from SCALANCE SC-600 family (https://support.industry.siemens.com/cs/document/109756957) and apply patches when available, or follow recommendations from section Workarounds and Mitigations See further recommendations from section Workarounds and Mitigations

SCALANCE S627-2M: All versions < V4.1	Update to V4.1 or later version Update is only available via Siemens Support Contact Upgrade hardware to successor product from SCALANCE SC-600 family (https://support.industry.siemens.com/cs/document/109756957) and apply patches when available, or follow recommendations from section Workarounds and Mitigations See further recommendations from section Workarounds and Mitigations
SCALANCE X-200 switch family (incl. SIPLUS NET variants): All versions < 5.2.4	Update to V5.2.4 or later version https://support.industry.siemens.com/cs/document/109767965/ See further recommendations from section Workarounds and Mitigations
SCALANCE X-200IRT switch family (incl. SIPLUS NET variants): All versions < V5.5.0	Update to V5.5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109792534/ 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 < 4.1.3	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:

- Only access links from trusted sources in the browser you use to configure the SCALANCE X switches.

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

The SCALANCE S-600 devices (S602, S612, S623, S627-2M) are used to protect trusted industrial networks from untrusted networks. The S-600 devices are superseded by the SCALANCE SC-600 devices (SC622-2C, SC632-2C, SC636-2C, SC642-2C, SC646-2C), or the SCALANCE S615.

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-2019-13924

The device does not send the X-Frame-Option Header in the administrative web interface, which makes it vulnerable to Clickjacking attacks.

The security vulnerability could be exploited by an attacker that is able to trick an administrative user with a valid session on the target device into clicking on a website controlled by the attacker. The vulnerability could allow an attacker to perform administrative actions via the web interface.

CVSS v3.1 Base Score	4.2
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:L/E:P/RL:U/RC:C
CWE	CWE-693: Protection Mechanism Failure

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 (2020-02-11):	Publication Date
V1.1 (2021-02-09):	Added solution for SCALANCE X-200IRT switch family
V1.2 (2021-04-13):	Added affected products SCALANCE S602, SCALANCE S612, SCALANCE S623, and SCALANCE S627-2M
V1.3 (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.