SSA-591405: Web Vulnerabilities in SCALANCE S-600 Family

Publication Date: 2020-02-11
Last Update: 2021-04-13
Current Version: V1.2
CVSS v3.1 Base Score: 7.5

SUMMARY

The firmware for SCALANCE S-600 family devices contains multiple web vulnerabilities. The vulnerabilities could allow an remote attacker to conduct Denial-of-Service attacks or perform Cross-Site Scripting attacks.

Siemens has released updates for the affected products and recommends to update to the latest versions, or to upgrade to a successor product.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE S602: All versions >= V3.0 and < V4.1	Update to V4.1 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
SCALANCE S612: All versions >= V3.0 and < V4.1	Update to V4.1 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
SCALANCE S623: All versions >= V3.0 and < V4.1	Update to V4.1 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

SCALANCE S627-2M: All versions >= V3.0 and < V4.1	Update to V4.1 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

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 access the SCALANCE S-600 administration website.

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.

The SCALANCE SC-600 devices (SC622-2C, SC632-2C, SC636-2C, SC642-2C, SC646-2C) are used to protect trusted industrial networks from untrusted networks. They allow filtering incoming and outgoing network connections in different ways.

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-2019-6585

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.

CVSS v3.1 Base Score	4.7
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

Vulnerability CVE-2019-13925

Specially crafted packets sent to port 443/tcp of affected devices could cause a Denial-of-Service condition of the web server.

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-400: Uncontrolled Resource Consumption

Vulnerability CVE-2019-13926

Specially crafted packets sent to port 443/tcp of affected devices could cause a Denial-of-Service condition of the web server. A cold reboot is required to restore the functionality of the device.

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-400: Uncontrolled Resource Consumption

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Melih Berk Ekşioğlu for coordinated disclosure of CVE-2019-6585

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 (2020-08-11):	Informed about successor products for the SCALANCE S-600 family
V1.2 (2021-04-13):	Added solution for SCALANCE S602, SCALANCE S612, SCALANCE S623, and SCALANCE S627-2M

TERMS OF USE

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.