SSA-242982: Cross-Site Scripting Vulnerability in SCALANCE S

Publication Date: 2018-11-13
Last Update: 2018-11-13
Current Version: V1.0
CVSS v3.0 Base Score: 4.7

SUMMARY

A Cross-Site Scripting (XSS) vulnerability was found in the web server of SCALANCE S firewalls. Siemens provides firmware version V4.0.1.1, which fixes the vulnerability and recommends to update to the newest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE S602: All versions < V4.0.1.1	Update to V4.0.1.1 https://support.industry.siemens.com/cs/document/109477325/-delivery-release-and-download-of-firmware-update-v4-0-1-1-for-scalance-s?dti=0&lc=en-WW
SCALANCE S612: All versions < V4.0.1.1	Update to V4.0.1.1 https://support.industry.siemens.com/cs/document/109477325/-delivery-release-and-download-of-firmware-update-v4-0-1-1-for-scalance-s?dti=0&lc=en-WW
SCALANCE S623: All versions < V4.0.1.1	Update to V4.0.1.1 https://support.industry.siemens.com/cs/document/109477325/-delivery-release-and-download-of-firmware-update-v4-0-1-1-for-scalance-s?dti=0&lc=en-WW
SCALANCE S627-2M: All versions < V4.0.1.1	Update to V4.0.1.1 https://support.industry.siemens.com/cs/document/109477325/-delivery-release-and-download-of-firmware-update-v4-0-1-1-for-scalance-s?dti=0&lc=en-WW

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 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 firewall is used to protect trusted industrial networks from untrusted networks. It allows 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 3.0 (CVSS v3.0) (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.

Vulnerability CVE-2018-16555

The integrated web server 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.

CVSS v3.0 Base Score	4.7
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Nelson Berg from Applied Risk for coordinated disclosure

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 (2018-11-13):	Publication Date

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.