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

Publication Date: 2018-06-12
Last Update: 2018-06-12
Current Version: V1.0
CVSS v3.0 Base Score: 5.8

SUMMARY

Two cross-site-scripting (XSS) vulnerabilities were found in the web server of SCALANCE X switches. Siemens recommends updating the firmware to the newest version as soon as possible.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE X-200: All versions < V5.2.3 only affected by CVE-2018-4848	Update to V5.2.3 https://support.industry.siemens.com/cs/ww/en/view/109758142
SCALANCE X-200 IRT: All versions < V5.4.1	Update to V5.4.1 https://support.industry.siemens.com/cs/ww/en/view/109758144
SCALANCE X300: All versions	See 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.

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).

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-2018-4842

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 v3.0 Base Score	5.5
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C

Vulnerability CVE-2018-4848

The integrated configuration web server of the affected Scalance X Switches 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 v3.0 Base Score	5.8
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C

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
- 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

TERMS OF USE