SSA-671286: Multiple Vulnerabilities in SCALANCE Products

Publication Date: 2019-08-13
Last Update: 2020-07-14
Current Version: V1.1
CVSS v3.1 Base Score: 6.6

SUMMARY

The latest updates for the below mentioned products contain fixes for multiple vulnerabilities. The most severe could allow authenticated local users with physical access to the device to execute arbitrary commands on the device under certain conditions.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE SC-600: V2.0	Update to V2.0.1 https://support.industry.siemens.com/cs/ww/en/view/109769665
SCALANCE XB-200: V4.1 only affected by CVE-2019-10927	Update to V4.2 https://support.industry.siemens.com/cs/ww/en/view/109779919/
SCALANCE XC-200: V4.1 only affected by CVE-2019-10927	Update to V4.2 https://support.industry.siemens.com/cs/ww/en/view/109779919/
SCALANCE XF-200BA: V4.1 only affected by CVE-2019-10927	Update to V4.2 https://support.industry.siemens.com/cs/ww/en/view/109779919/
SCALANCE XP-200: V4.1 only affected by CVE-2019-10927	Update to V4.2 https://support.industry.siemens.com/cs/ww/en/view/109779919/
SCALANCE XR-300WG: V4.1 only affected by CVE-2019-10927	Update to V4.2 https://support.industry.siemens.com/cs/ww/en/view/109779919/

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Protect access to port 22/tcp (using the build-in firewall for SCALANCE SC-600)
- Protect physical access to the device

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 SC firewall is used to protect trusted industrial networks from untrusted networks. It allows filtering incoming and outgoing network connections in different ways.

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 3.1 (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-2019-10927

An authenticated attacker with network access to to port 22/tcp of an affected device may cause a Denial-of-Service condition.

The security vulnerability could be exploited by an authenticated attacker with network access to the affected device. No user interaction is required to exploit this vulnerability. The vulnerability impacts the availability of the affected device.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-703: Improper Check or Handling of Exceptional Conditions

Vulnerability CVE-2019-10928

An authenticated attacker with access to port 22/tcp as well as physical access to an affected device may trigger the device to allow execution of arbitrary commands.

The security vulnerability could be exploited by an authenticated attacker with physical access to the affected device. No user interaction is required to exploit this vulnerability. The vulnerability impacts the confidentiality, integrity and availability of the affected device.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-703: Improper Check or Handling of Exceptional Conditions

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 (2019-08-13):	Publication Date
V1.1 (2020-07-14):	Added solution for SCALANCE XB-200, XC-200, XP-200,XF-200BA and XR-300WG

TERMS OF USE