

SSA-671286: Multiple Vulnerabilities in SCALANCE Products

Publication Date: 2019-08-13
Last Update: 2019-08-13
Current Version: V1.0
CVSS v3.0 Base Score: 6.6

SUMMARY

The latest update for SCALANCE SC-600 fixes 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 SCALANCE SC-600 devices.

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	See recommendations from section Workarounds and Mitigations
SCALANCE XC-200: V4.1 only affected by CVE-2019-10927	See recommendations from section Workarounds and Mitigations
SCALANCE XF-200BA: V4.1 only affected by CVE-2019-10927	See recommendations from section Workarounds and Mitigations
SCALANCE XP-200: V4.1 only affected by CVE-2019-10927	See recommendations from section Workarounds and Mitigations
SCALANCE XR-300WG: V4.1 only affected by CVE-2019-10927	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:

- 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 3.0 (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-2019-10927

An authenticated attacker with network access 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 v3.0 Base Score	6.5
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C

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 v3.0 Base Score	6.6
CVSS Vector	CVSS:3.0/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

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

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.