

SSA-676336: OpenSSH Vulnerabilities in SCALANCE X-200 and X-300/X408 Switches

Publication Date: 2021-09-14
Last Update: 2021-09-14
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

The latest update of the SCALANCE X-200 and X-300/X408 switches families fixes multiple OpenSSH vulnerabilities. The most severe of these vulnerabilities could allow a denial of service condition.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE X200-4P IRT: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X201-3P IRT: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X201-3P IRT PRO: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X202-2 IRT: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X202-2P IRT (incl. SIPLUS NET variant): All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X202-2P IRT PRO: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X204 IRT: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X204 IRT PRO: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X204-2 (incl. SIPLUS NET variant): All Versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X204-2FM: All Versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/

SCALANCE X204-2LD (incl. SIPLUS NET variant): All Versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X204-2LD TS: All Versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X204-2TS: All Versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X206-1: All Versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X206-1LD: All Versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X208 (incl. SIPLUS NET variant): All Versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X208PRO: All Versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X212-2 (incl. SIPLUS NET variant): All Versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X212-2LD: All Versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X216: All Versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X224: All Versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X302-7 EEC: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X304-2FE: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X306-1LD FE: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X307-3: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X307-3LD: All versions	See recommendations from section Workarounds and Mitigations

SCALANCE X308-2 (incl. SIPLUS NET variant): All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X308-2LD: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH+: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X308-2M: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X308-2M PoE: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X308-2M TS: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X310: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X310FE: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X320-1 FE: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X320-1-2LD FE: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X408-2: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XF201-3P IRT: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XF202-2P IRT: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XF204: All Versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE XF204 IRT: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XF204-2 (incl. SIPLUS NET variant): All Versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE XF204-2BA IRT: All versions	See recommendations from section Workarounds and Mitigations

SCALANCE XF206-1: All Versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE XF208: All Versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE XR324-4M EEC: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE TS: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M TS: 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:

- Monitor and restrict access to port 22/TCP
- Disable SCALANCE SSH setting, if possible in your environment. SSH port status is open by default

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 (HMI).

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

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-2016-6515

The `auth_password` function in `auth-passwd.c` in `sshd` in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.

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:U/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2016-10011

`authfile.c` in `sshd` in OpenSSH before 7.4 does not properly consider the effects of `realloc` on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C
CWE	CWE-264: Permissions, Privileges, and Access Controls

Vulnerability CVE-2016-10708

`sshd` in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence `NEWKEYS` message, as demonstrated by Honggfuzz, related to `kex.c` and `packet.c`.

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:U/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

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 (2021-09-14): 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.