SSA-479249: Weak Encryption Vulnerability in SCALANCE X-200IRT Devices

Publication Date: 2023-04-11
Last Update: 2023-04-11
Current Version: V1.0
CVSS v3.1 Base Score: 6.7

SUMMARY

The SSH server on SCALANCE X-200IRT devices is configured to offer weak ciphers by default. This could allow an unauthorized attacker in a man-in-the-middle position to read and modify any data passed over the connection between legitimate clients and the affected device.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE X200-4P IRT (6GK5200-4AH00-2BA3): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/ See recommendations from section Workarounds and Mitigations
SCALANCE X201-3P IRT (6GK5201-3BH00-2BA3): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/ See recommendations from section Workarounds and Mitigations
SCALANCE X201-3P IRT PRO (6GK5201-3JR00-2BA6): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/ See recommendations from section Workarounds and Mitigations
SCALANCE X202-2IRT (6GK5202-2BB00-2BA3): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/ See recommendations from section Workarounds and Mitigations
SCALANCE X202-2IRT (6GK5202-2BB10-2BA3): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/ See recommendations from section Workarounds and Mitigations
SCALANCE X202-2P IRT (6GK5202-2BH00-2BA3): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/ See recommendations from section Workarounds and Mitigations

SCALANCE X202-2P IRT PRO (6GK5202-2JR00-2BA6): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/ See recommendations from section Workarounds and Mitigations
SCALANCE X204IRT (6GK5204-0BA00-2BA3): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/ See recommendations from section Workarounds and Mitigations
SCALANCE X204IRT (6GK5204-0BA10-2BA3): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/ See recommendations from section Workarounds and Mitigations
SCALANCE X204IRT PRO (6GK5204-0JA00-2BA6): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/ See recommendations from section Workarounds and Mitigations
SCALANCE XF201-3P IRT (6GK5201-3BH00-2BD2): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/ See recommendations from section Workarounds and Mitigations
SCALANCE XF202-2P IRT (6GK5202-2BH00-2BD2): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/ See recommendations from section Workarounds and Mitigations
SCALANCE XF204-2BA IRT (6GK5204-2AA00-2BD2): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/ See recommendations from section Workarounds and Mitigations
SCALANCE XF204IRT (6GK5204-0BA00-2BF2): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/ See recommendations from section Workarounds and Mitigations
SIPLUS NET SCALANCE X202-2P IRT (6AG1202-2BH00-2BA3): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/ 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:

- Configure the SSH clients to make use of the following strong key exchange ciphers
- Add only trusted SSH client public keys to ROS and allow access to those clients only

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

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).

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-2023-29054

The SSH server on affected devices is configured to offer weak ciphers by default.

This could allow an unauthorized attacker in a man-in-the-middle position to read and modify any data passed over the connection between legitimate clients and the affected device.

CVSS v3.1 Base Score	6.7
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-326: Inadequate Encryption Strength

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 (2023-04-11): 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.