

SSA-274900: Use of Hardcoded Key in SCALANCE X Devices Under Certain Conditions

Publication Date: 2021-01-12
 Last Update: 2022-12-13
 Current Version: V1.3
 CVSS v3.1 Base Score: 9.1

SUMMARY

SCALANCE X devices might not generate a unique random key after factory reset, and use a private key shipped with the firmware.

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 X-200 switch family (incl. SIPLUS NET variants): All versions < V5.2.5 only affected by CVE-2020-28391 | Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/ See further recommendations from section Workarounds and Mitigations |
| SCALANCE X-200IRT switch family (incl. SIPLUS NET variants): All versions < V5.5.0 only affected by CVE-2020-28391 | Update to V5.5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109792534/ See further recommendations from section Workarounds and Mitigations |
| SCALANCE X-200RNA switch family: All versions < V3.2.7 | Update to V3.2.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109814809/ See further recommendations from section Workarounds and Mitigations |
| SCALANCE X-300 switch family (incl. X408 and SIPLUS NET variants): All versions < V4.1.0 only affected by CVE-2020-28395 | Update to V4.1.0 or later version (for supported devices) https://support.industry.siemens.com/cs/ww/en/view/109773547/ See further 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:

- Update the default selfsigned device X.509 certificates with own trusted certificates
- Update the default hardcoded X.509 certificates from the firmware image (fingerprints SHA-1: **F2:C8:3B:8F:86:27:74:AA:60:EC:D4:A0:CF:0D:BE:A6:D1:FE:22:12** and SHA-256: **25:60:DB:B3:F9:07:9D:69:0E:DD:A9:EB:4E:1C:D5:8E:AF:79:16:C3:C8:13:A6:F6:59:AD:05:E4:6F:77:F7:72** - fingerprints for X-200RNA switch devices SHA-1: **04:64:EF:98:A4:42:D2:BB:57:4A:47:12:20:EC:E6:85:15:4F:03:61** and SHA-256: **9C:15:FA:56:ED:FF:CA:8D:17:16:E9:2C:57:CB:90:3C:4E:81:5B:3D:60:E9:CF:26:07:B3:73:F6:C7:02:75:88**)

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-2020-28391

Devices create a new unique key upon factory reset, except when used with C-PLUG. When used with C-PLUG the devices use the hardcoded private RSA-key shipped with the firmware-image. An attacker could leverage this situation to a man-in-the-middle situation and decrypt previously captured traffic.

| | |
|----------------------|--|
| CVSS v3.1 Base Score | 9.1 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:U/RC:C |
| CWE | CWE-321: Use of Hard-coded Cryptographic Key |

Vulnerability CVE-2020-28395

Devices do not create a new unique private key after factory reset. An attacker could leverage this situation to a man-in-the-middle situation and decrypt previously captured traffic.

| | |
|----------------------|--|
| CVSS v3.1 Base Score | 9.1 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:U/RC:C |
| CWE | CWE-321: Use of Hard-coded Cryptographic Key |

ADDITIONAL INFORMATION

These vulnerabilities have been discovered internally by Siemens.

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 (2021-01-12): | Publication Date |
| V1.1 (2021-02-09): | Added update information for SCALANCE X-200IRT switch family |
| V1.2 (2021-09-14): | Added solution for SCALANCE X-200 switch family |
| V1.3 (2022-12-13): | Added SCALANCE X-200RNA switch family |

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.