SSA-646841: Recoverable Password from Configuration Storage in SCALANCE X Switches

Publication Date:	2019-06-11
Last Update:	2021-02-09
Current Version:	V1.2
CVSS v3.1 Base Score:	7.1

SUMMARY

A vulnerability exists in several SCALANCE X switches that could allow external entities to reconstruct passwords for users of the affected devices if an attacker is able to obtain a backup of the device configuration.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE X-200 switch family (incl. SIPLUS NET variants): All Versions < V5.2.4	Update to V5.2.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109767965
SCALANCE X-200IRT switch family (incl. SIPLUS NET variants): All versions < V5.5.0	Update to V5.5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109792534/
SCALANCE X-300 switch family (incl. X408 and SIPLUS NET variants): All versions < V4.1.3	Update to V4.1.3 or later version https://support.industry.siemens.com/cs/document/109773547
SCALANCE X-414-3E: 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:

- Restrict access to config backups or archived device configuration files
- Restrict or disable network access to mechanisms that allow to retrieve the device configuration, if enabled.
- Restrict access to device configuration module C-PLUG, if in use.
- SCALANCE X-414-3E: Migrate to SCALANCE XM-400 product line

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-2019-6567

The affected devices store passwords in a recoverable format. An attacker may extract and recover device passwords from the device configuration.

Successful exploitation requires access to a device configuration backup and impacts confidentiality of the stored passwords.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-257: Storing Passwords in a Recoverable Format

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Christopher Wade from Pen Test Partners for coordinated disclosure
- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

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 (2019-06-11): Publication Date
V1.1 (2020-01-14): SIPLUS devices now explicitly mentioned in the list of affected products; added update information for SCALANCE X-300/X408
V1.2 (2021-02-09): Added solution for SCALANCE X-200IRT 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.