SSA-170686: Vulnerabilities in SCALANCE X-200 and X-200IRT Switch Families

Publication Date:	2013-05-24
Last Update:	2019-12-10
Current Version:	V1.2
CVSS v3.1 Base Score:	7.6

SUMMARY

Two vulnerabilities have been reported for the Siemens SCALANCE X-200 and X-200IRT switch families concerning a privilege escalation bug in the web interface and an authentication problem in the SNMPv3 implementation. Siemens has addressed both vulnerabilities by firmware upgrades.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE X-200 switch family (incl. SIPLUS NET variants): Versions < V5.0.0 for CVE-2013-3633 and versions < V4.5.0 for CVE-2013-3634	Update to V5.0.0 (released in 2013), or any later version (currently V5.2.4) https://support.industry.siemens.com/cs/document/109767965
SCALANCE X-200IRT switch family (incl. SIPLUS NET variants): All versions < V5.1.0	Update to V5.1.0 (released in 2013), or any later version (currently V5.4.2) https://support.industry.siemens.com/cs/document/109763309

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Disable SNMPv3 completely to mitigate CVE-2013-3634

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-2013-3633

The user privileges for the web interface are only enforced on client side and not properly verified on server side. Therefore, an attacker is able to execute privileged commands using an unprivileged account.

CVSS v3.1 Base Score	7.6
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C
CWE	CWE-603: Use of Client-Side Authentication

Vulnerability CVE-2013-3634

The implementation of SNMPv3 does not check the user credentials sufficiently. Therefore, an attacker is able to execute SNMP commands without correct credentials.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-287: Improper Authentication

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Hay Mizrachi from OTORIO for reporting CVE-2013-3633 also for Scalance X-200 switch family
- 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 (2013-05-24):	Publication Date

V1.1 (2013-05-27):	Adjusted CVSS Base Score from 6.4 to 7.5 for CVE-2013-3634
V1.2 (2019-12-10):	Added Scalance X-200 switch family; revised summary; updated CVSS Scores from CVSSv2 to CVSSv3.1; SIPLUS devices now explicitly mentioned in the list of affected products

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.