SSA-954136: User Impersonation Vulnerability in SCALANCE X-200IRT Switch Family

Publication Date: 2015-02-02
Last Update: 2020-02-10
Current Version: V1.1
CVSS v3.1 Base Score: 6.3

SUMMARY

The latest firmware update for the SCALANCE X-200IRT switch family fixes a vulnerability which could allow attackers to impersonate legitimate users of the web interface.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE X-200IRT switch family (incl. SIPLUS NET variants) Products with the following MLFBs are affected: 6GK5201-3BH00-2BA3 6GK5200-4AH00-2BA3 6GK5202-2BB00-2BA3 6GK5204-0BA00-2BA3 6GK5201-3JR00-2BA6 6GK5204-0BA00-2BF2 6GK5204-0JA00-2BA6 6GK5202-2JR00-2BA6 6GK5202-2BH00-2BA3: All versions < V5.2.0	Firmware version V5.2.0 https://support.industry.siemens.com/cs/ww/en/view/109744096

WORKAROUNDS AND MITIGATIONS

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

- Operate the device only within trusted networks

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-2015-1049

The device's web server could allow unauthenticated attackers to impersonate legitimate users of the web interface (port 80/tcp and port 443/tcp) if an active web session of an authenticated user exists at the time of attack.

CVSS v3.1 Base Score	6.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/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:

- 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 (2015-02-02): Publication Date
V1.1 (2020-02-10): SIPLUS devices now explicitly mentioned in the list of affected products

TERMS OF USE