SSA-443566: Authentication Bypass in SCALANCE X Switches Families

Publication Date: 2020-01-14
Last Update: 2020-01-14
Current Version: V1.0
CVSS v3.1 Base Score: 8.8

SUMMARY

Several SCALANCE X switches are affected by an Authentication Bypass vulnerability. The vulnerability allows an unauthenticated attacker to violate access-control rules. The vulnerability can be exploited by sending a GET request to a specific uniform resource locator on the web configuration interface of the device.

The security vulnerability could be exploited by an attacker with network access to the affected systems. An attacker could use the vulnerability to obtain sensitive information or change the device configuration.

Siemens recommends to upgrade the SCALANCE X-300 and X408 switches to firmware version V4.1.3.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE X-200RNA switch family: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X-300 switch family (incl. X408 and SIPLUS NET variants): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547

WORKAROUNDS AND MITIGATIONS

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

- Configure ACLs to only allow Web-based management from trusted IP Adresses
- Disable web-based management (WBM) and use SSH to configure the device

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-2019-13933

Affected devices contain a vulnerability that allows an unauthenticated attacker to violate access-control rules. The vulnerability can be triggered by sending GET request to specific uniform resource locator on the web configuration interface of the device.

The security vulnerability could be exploited by an attacker with network access to the affected systems. An attacker could use the vulnerability to obtain sensitive information or change the device configuration.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Maxim Rupp for coordinated disclosure

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 (2020-01-14): Publication Date

TERMS OF USE