SSA-100232: Denial-of-Service vulnerability in SCALANCE X switches

Publication Date: 2019-08-13
Last Update: 2019-08-13
Current Version: V1.0
CVSS v3.0 Base Score: 8.6

SUMMARY

A vulnerability in the affected devices could allow an unauthenticated attacker with network access to an affected device to perform a denial-of-service.

Siemens is preparing updates and recommends specific countermeasures until patches are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE X-200: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X-200IRT: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X-200RNA: 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:

- Disable telnet service on affected devices. Customers should use SSH instead.
- Restrict network access to port 23/tcp of 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).

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

Vulnerability CVE-2019-10942

The device contains a vulnerability that could allow an attacker to trigger a denial-of-service condition by sending large message packages repeatedly to the telnet service.

The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the device.

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

CVSS v3.0 Base Score	8.6
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:T/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Younes Dragoni and Alessandro Di Pinto from Nozomi Networks for reporting the vulnerability.

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 (2019-08-13): Publication Date

TERMS OF USE