SSA-557804: Mirror Port Isolation Vulnerability in SCALANCE X Switches

Publication Date: 2019-03-12
Last Update: 2020-01-14
Current Version: V1.2
CVSS v3.1 Base Score: 5.4

SUMMARY

A vulnerability was identified in several SCALANCE X switches that could allow an attacker to feed information into a network via the mirror port with the monitor barrier feature enabled.

The monitor barrier implementation in several SCALANCE X switches does allow traffic to be directed back into the mirroring network. This might allow an attacker to feed back information into the network that is mirrored.

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 https://support.industry.siemens.com/cs/ww/en/view/109767965
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
SCALANCE XP/XC/XF-200 switch family (incl. SIPLUS NET variants): All versions < V4.1	Update to V4.1 https://support.industry.siemens.com/cs/ww/en/view/109762982

WORKAROUNDS AND MITIGATIONS

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

- Apply defense in depth principles, in particular make sure that no devices that transmit data back into the mirroring network are operated within the mirrored network

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-2019-6569

The monitor barrier of the affected products insufficiently blocks data from being forwarded over the mirror port into the mirrored network. An attacker might use this behaviour to transmit malicious packets to systems in the mirrored network, possibly influencing their configuration and runtime behaviour.

The security vulnerability could be exploited by an attacker with network access to the traffic-receiving network. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise the confidentiality and availability of the traffic-generating network.

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

CVSS v3.1 Base Score	5.4
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-440: Expected Behavior Violation

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 (2019-03-12):	Publication date
V1.1 (2019-06-11):	Added update information for Scalance X-200
V1.2 (2020-01-14):	SIPLUS devices now explicitly mentioned in the list of affected products; added update information for SCALANCE X-300/X408

TERMS OF USE