

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

Publication Date: 2019-03-12
Last Update: 2019-03-12
Current Version: V1.0
CVSS v3.0 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 various SCALANCE products 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: All versions	See recommendations from section Workarounds and Mitigations
Scalance X-300: All versions	See recommendations from section Workarounds and Mitigations
Scalance XP/XC/XF-200: 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).

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-2019-6569

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 v3.0 Base Score	5.4
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:L/E:P/RL:O/RC:C

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

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.