SSA-116379: Denial-of-Service Vulnerability in OSPF Packet Handling of SCALANCE XM-400 and XR-500 Devices

Publication Date: 2021-05-11
Last Update: 2021-05-11
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

SCALANCE XM-400 and XR-500 devices contain a vulnerability in the OSPF protocol implementation that could allow an unauthenticated remote attacker to create a permanent denial-of-service condition.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE XM-400 Family: All versions < V6.4	Update to V6.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109796319/
SCALANCE XR-500 Family: All versions < V6.4	Update to V6.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109796317/

WORKAROUNDS AND MITIGATIONS

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

- Disable OSPF in the layer 3 configuration menu (note that OSPF is disabled by default). The vulnerability is not exploitable, when OSPF is disabled.
- If OSPF is used, set a password for the OSPF interface and enable MD5 authentication

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 3.1 (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-2020-28393

The OSPF protocol implementation in affected devices incorrectly handles the number of LSA fields in combination with other modified fields.

An unauthenticated remote attacker could create a permanent denial-of-service condition by sending specially crafted OSPF packets. Successful exploitation requires OSPF to be enabled on an affected device.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-682: Incorrect Calculation

ADDITIONAL INFORMATION

All SCALANCE XM-400 and XR-500 devices are affected, including those who do not support layer 3 routing and OSPF natively, as the activation of these features is possible via the KEY-PLUG modules:

- KEY-PLUG for XM-400: https://mall.industry.siemens.com/mall/en/de/Catalog/Product/6GK5904-0PA00
- KEY-PLUG for XR-500: https://mall.industry.siemens.com/mall/en/de/Catalog/Product/6GK5905-0PA00

As long as layer 3 routing including OSPF is not enabled, the vulnerability is not exploitable.

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 (2021-05-11): Publication Date

TERMS OF USE