SSA-145224: Vulnerability in OSPF Packet Handling of SCALANCE XM-400 and XR-500 Devices

Publication Date: 2022-06-14
Last Update: 2022-06-14
Current Version: V1.0
CVSS v3.1 Base Score: 5.9

SUMMARY

SCALANCE XM-400 and XR-500 devices contain a vulnerability in the OSPF protocol implementation that could allow an unauthenticated remote attacker to cause interruptions in the network.

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 XM408-4C (6GK5408-4GP00-2AM2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XM408-4C (L3 int.) (6GK5408-4GQ00-2AM2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XM408-8C (6GK5408-8GS00-2AM2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XM408-8C (L3 int.) (6GK5408-8GR00-2AM2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XM416-4C (6GK5416-4GS00-2AM2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XM416-4C (L3 int.) (6GK5416-4GR00-2AM2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR524-8C, 1x230V (6GK5524-8GS00-3AR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR524-8C, 1x230V (L3 int.) (6GK5524-8GR00-3AR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR524-8C, 2x230V (6GK5524-8GS00-4AR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR524-8C, 2x230V (L3 int.) (6GK5524-8GR00-4AR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR524-8C, 24V (6GK5524-8GS00-2AR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR524-8C, 24V (L3 int.) (6GK5524-8GR00-2AR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR526-8C, 1x230V (6GK5526-8GS00-3AR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR526-8C, 1x230V (L3 int.) (6GK5526-8GR00-3AR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR526-8C, 2x230V (6GK5526-8GS00-4AR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR526-8C, 2x230V (L3 int.) (6GK5526-8GR00-4AR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR526-8C, 24V (6GK5526-8GS00-2AR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR526-8C, 24V (L3 int.) (6GK5526-8GR00-2AR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR528-6M (6GK5528-0AA00-2AR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR528-6M (2HR2) (6GK5528-0AA00-2HR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR528-6M (2HR2, L3 int.) (6GK5528-0AR00-2HR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR528-6M (L3 int.) (6GK5528-0AR00-2AR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR552-12M (6GK5552-0AA00-2AR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR552-12M (2HR2) (6GK5552-0AA00-2HR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR552-12M (2HR2) (6GK5552-0AR00-2HR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR552-12M (2HR2, L3 int.) (6GK5552-0AR00-2AR2): All versions < V6.5	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/ See further 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 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

Product specific remediations or mitigations can be found in the section Affected Products and Solution.

Please follow the General Security Recommendations.

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-2021-37182

The OSPF protocol implementation in affected devices fails to verify the checksum and length fields in the OSPF LS Update messages.

An unauthenticated remote attacker could exploit this vulnerability to cause interruptions in the network by sending specially crafted OSPF packets. Successful exploitation requires OSPF to be enabled on an affected device.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-354: Improper Validation of Integrity Check Value

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 (2022-06-14): Publication Date

TERMS OF USE