

SSA-979775: Stack Overflow Vulnerability in SCALANCE and RUGGEDCOM Devices

Publication Date: 2021-03-09
 Last Update: 2021-03-09
 Current Version: V1.0
 CVSS v3.1 Base Score: 8.8

SUMMARY

Several firmware versions of the SCALANCE and RUGGEDCOM devices listed below are affected by a vulnerability in the passive listening feature that could allow an attacker to cause a reboot or, under specific circumstances, attain remote code execution of the affected devices.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|--|--|
| RUGGEDCOM RM1224: All versions >= V4.3 | See recommendations from section Workarounds and Mitigations |
| SCALANCE M-800: All versions >= V4.3 | See recommendations from section Workarounds and Mitigations |
| SCALANCE S615: All versions >= V4.3 | See recommendations from section Workarounds and Mitigations |
| SCALANCE SC-600 Family: All versions >= V2.0 and < V2.1.3 | Update to V2.1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109793041/ |
| SCALANCE X300WG: All versions < V4.1 | Update to V4.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109773547/ |
| SCALANCE XM400: All versions < V6.2 | Update to V6.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109764409/ |
| SCALANCE XR500: All versions < V6.2 | Update to V6.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109761425/ |
| SCALANCE Xx200 Family: All versions < V4.1 | Update to V4.1 or later version 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:

- Deactivate the STP passive listening feature of the vulnerable devices

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

The SCALANCE SC-600 devices (SC622-2C, SC632-2C, SC636-2C, SC642-2C, SC646-2C) are used to protect trusted industrial networks from untrusted networks. They allow filtering incoming and outgoing network connections in different ways.

The SCALANCE M-800 / S615 industrial routers are used for secure remote access to plants via mobile networks, e.g. GPRS or UMTS with the integrated security functions of a firewall for protection against unauthorized access and VPN to protect data transmission.

SCALANCE X switches are used to connect industrial components like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs).

RUGGEDCOM RM1224 is a 4G ROUTER for wireless IP-communication from Ethernet based devices via LTE(4G)- mobile radio.

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-2021-25667

Affected devices contain a stack-based buffer overflow vulnerability in the handling of STP BPDU frames that could allow a remote attacker to trigger a denial-of-service condition or potentially remote code execution.

Successful exploitation requires the passive listening feature of the device to be active.

| | |
|----------------------|--|
| CVSS v3.1 Base Score | 8.8 |
| CVSS Vector | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-121: Stack-based Buffer Overflow |

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 (2021-03-09): 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.