# SSA-697140: Denial of Service Vulnerability in the TCP Event Service of SCALANCE and RUGGEDCOM Products

Publication Date: 2022-10-11
Last Update: 2023-03-14
Current Version: V1.2
CVSS v3.1 Base Score: 8.6

## SUMMARY

The products listed below contain a denial of service vulnerability in the TCP event interface that could allow an unauthenticated remote attacker to render the device unusable.

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 |
|---|---|
| RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See further recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M804PB (6GK5804-0AP00-2AA2):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M812-1 ADSL-Router (Annex A) (6GK5812-1AA00-2AA2):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M812-1 ADSL-Router (Annex B) (6GK5812-1BA00-2AA2):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M816-1 ADSL-Router (Annex A) (6GK5816-1AA00-2AA2):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE M816-1 ADSL-Router (Annex B) (6GK5816-1BA00-2AA2):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M874-2 (6GK5874-2AA00-2AA2):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M874-3 (6GK5874-3AA00-2AA2):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M876-3 (EVDO) (6GK5876-3AA02-2BA2):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M876-4 (6GK5876-4AA10-2BA2):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE S615 (6GK5615-0AA00-2AA2):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE S615 EEC (6GK5615-0AA01-2AA2):<br>All versions < V7.1.2 | Update to V7.1.2 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109813051/<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE WAM763-1 (6GK5763-1AL00-7DA0):<br>All versions >= V1.1.0 < V2.0 | Update to V2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109815650/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE WAM766-1 (EU) (6GK5766-1GE00-7DA0):<br>All versions >= V1.1.0 < V2.0 | Update to V2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109815650/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE WAM766-1 (US) (6GK5766-1GE00-7DB0):<br>All versions >= V1.1.0 < V2.0 | Update to V2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109815650/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE WAM766-1 EEC (EU) (6GK5766-1GE00-7TA0):<br>All versions >= V1.1.0 < V2.0 | Update to V2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109815650/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE WAM766-1 EEC (US) (6GK5766-1GE00-7TB0):<br>All versions >= V1.1.0 < V2.0 | Update to V2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109815650/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE WUM763-1 (6GK5763-1AL00-3AA0):<br>All versions >= V1.1.0 < V2.0 | Update to V2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109815650/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE WUM763-1 (6GK5763-1AL00-3DA0):<br>All versions >= V1.1.0 < V2.0 | Update to V2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109815650/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE WUM766-1 (EU) (6GK5766-1GE00-3DA0):<br>All versions >= V1.1.0 < V2.0 | Update to V2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109815650/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE WUM766-1 (US) (6GK5766-1GE00-3DB0):<br>All versions >= V1.1.0 < V2.0 | Update to V2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109815650/<br>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:

- Deactivate the TCP Event feature (not active by default)
- Restrict access to the TCP Event Service port (default 26864/tcp) to trusted networks and client IP addresses

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 M-800, MUM-800 and S615 as well as the RUGGEDCOM RM1224 are industrial routers.

SCALANCE W-700 products are wireless communication devices based on IEEE 802.11ax or 802.11n standard. They are used to connect all to sorts of WLAN devices (Access Points or Clients, depending on the operating mode) with a strong focus on industrial components, like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs) and others.

## 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-2022-31766

Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service condition and reboot the device thus possibly affecting other network resources.

| | |
|---|---|
| CVSS v3.1 Base Score | 8.6 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-20: Improper Input Validation |

## ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Martin Grubhofer and Michael Messner from Siemens Energy for reporting the vulnerability

## 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 (2022-10-11): | Publication Date |
| V1.1 (2023-01-10): | Added fix for SCALANCE W-700 IEEE 802.11ax product family |
| V1.2 (2023-03-14): | Added missing affected products SCALANCE S615 EEC (6GK5615-0AA01-2AA2) and SCALANCE M876-4 (6GK5876-4AA10-2BA2) |

## TERMS OF USE

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.