SSA-068047: Multiple Vulnerabilities in SCALANCE M-800 Family Before V7.2.2

Publication Date: 2023-12-12
Last Update: 2024-08-13
Current Version: V1.1
CVSS v3.1 Base Score: 7.2

SUMMARY

SCALANCE M-800 family before V7.2.2 is affected by multiple vulnerabilities.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE M-800 family (incl. S615, MUM-800 and RM1224):	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
RUGGEDCOM RM1224 family (6GK6108-4AM00):	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE M-800 family:	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE M804PB (6GK5804-0AP00-2AA2): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE M812-1 ADSL-Router family:	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/

SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE M816-1 ADSL-Router family:	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE M874-2 (6GK5874-2AA00-2AA2): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE M874-3 (6GK5874-3AA00-2AA2): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE M876-3 (6GK5876-3AA02-2BA2): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE M876-4 (6GK5876-4AA10-2BA2): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/

SCALANCE MUM-800 family:	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE S615 family:	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/
SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2): All versions < V7.2.2 affected by all CVEs	Update to V7.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822615/

WORKAROUNDS AND MITIGATIONS

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.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2023-44317

Affected products do not properly validate the content of uploaded X509 certificates which could allow an attacker with administrative privileges to execute arbitrary code on the device.

CVSS v3.1 Base Score	7.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data

Vulnerability CVE-2023-44320

Affected devices do not properly validate the authentication when performing certain modifications in the web interface allowing an authenticated attacker to influence the user interface configured by an administrator.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-425: Direct Request ('Forced Browsing')

Vulnerability CVE-2023-49692

An Improper Neutralization of Special Elements used in an OS Command with root privileges vulnerability exists in the parsing of the IPSEC configuration. This could allow malicious local administrators to issue commands on system level after a new connection is established.

CVSS v3.1 Base Score	7.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

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 (2023-12-12): Publication Date
V1.1 (2024-08-13): Add CVE-2023-44320 as fixed in V7.2.2

TERMS OF USE