

## SSA-180704: Multiple Vulnerabilities in SCALANCE M-800 Family Before V8.0

Publication Date: 2023-12-12  
 Last Update: 2024-08-13  
 Current Version: V1.1  
 CVSS v3.1 Base Score: 9.1  
 CVSS v4.0 Base Score: 9.4

### SUMMARY

SCALANCE M-800 family before V8.0 is affected by multiple vulnerabilities.

Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens recommends countermeasures for products where fixes are not, or not yet available.

### AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE M-800 family (incl. S615, MUM-800 and RM1224):	See below
RUGGEDCOM RM1224 family (6GK6108-4AM00):	See below
RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2):	See below
RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2): All versions < V8.0 affected by <a href="#">CVE-2022-46143</a> , <a href="#">CVE-2023-44319</a> , <a href="#">CVE-2023-44322</a> , <a href="#">CVE-2023-44373</a> , <a href="#">CVE-2023-44374</a> , <a href="#">CVE-2023-49691</a>	Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a>
RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2): All versions affected by <a href="#">CVE-2023-44318</a>	Currently no fix is planned
RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2):	See below
RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2): All versions < V8.0 affected by <a href="#">CVE-2022-46143</a> , <a href="#">CVE-2023-44319</a> , <a href="#">CVE-2023-44322</a> , <a href="#">CVE-2023-44373</a> , <a href="#">CVE-2023-44374</a> , <a href="#">CVE-2023-49691</a>	Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a>

RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2): All versions affected by <a href="#">CVE-2023-44318</a>	Currently no fix is planned
SCALANCE M-800 family:	See below
SCALANCE M804PB (6GK5804-0AP00-2AA2):	See below
SCALANCE M804PB (6GK5804-0AP00-2AA2): All versions < V8.0 affected by <a href="#">CVE-2022-46143</a> , <a href="#">CVE-2023-44319</a> , <a href="#">CVE-2023-44322</a> , <a href="#">CVE-2023-44373</a> , <a href="#">CVE-2023-44374</a> , <a href="#">CVE-2023-49691</a>	Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a>
SCALANCE M804PB (6GK5804-0AP00-2AA2): All versions affected by <a href="#">CVE-2023-44318</a>	Currently no fix is planned
SCALANCE M812-1 ADSL-Router family:	See below
SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2):	See below
SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2): All versions < V8.0 affected by <a href="#">CVE-2022-46143</a> , <a href="#">CVE-2023-44319</a> , <a href="#">CVE-2023-44322</a> , <a href="#">CVE-2023-44373</a> , <a href="#">CVE-2023-44374</a> , <a href="#">CVE-2023-49691</a>	Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a>
SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2): All versions affected by <a href="#">CVE-2023-44318</a>	Currently no fix is planned
SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2):	See below
SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2): All versions < V8.0 affected by <a href="#">CVE-2022-46143</a> , <a href="#">CVE-2023-44319</a> , <a href="#">CVE-2023-44322</a> , <a href="#">CVE-2023-44373</a> , <a href="#">CVE-2023-44374</a> , <a href="#">CVE-2023-49691</a>	Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a>
SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2): All versions affected by <a href="#">CVE-2023-44318</a>	Currently no fix is planned
SCALANCE M816-1 ADSL-Router family:	See below

SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2):	See below
SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2): All versions < V8.0 affected by <a href="#">CVE-2022-46143</a> , <a href="#">CVE-2023-44319</a> , <a href="#">CVE-2023-44322</a> , <a href="#">CVE-2023-44373</a> , <a href="#">CVE-2023-44374</a> , <a href="#">CVE-2023-49691</a>	Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a>
SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2): All versions affected by <a href="#">CVE-2023-44318</a>	Currently no fix is planned
SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2):	See below
SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2): All versions < V8.0 affected by <a href="#">CVE-2022-46143</a> , <a href="#">CVE-2023-44319</a> , <a href="#">CVE-2023-44322</a> , <a href="#">CVE-2023-44373</a> , <a href="#">CVE-2023-44374</a> , <a href="#">CVE-2023-49691</a>	Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a>
SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2): All versions affected by <a href="#">CVE-2023-44318</a>	Currently no fix is planned
SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2):	See below
SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2): All versions < V8.0 affected by <a href="#">CVE-2022-46143</a> , <a href="#">CVE-2023-44319</a> , <a href="#">CVE-2023-44322</a> , <a href="#">CVE-2023-44373</a> , <a href="#">CVE-2023-44374</a> , <a href="#">CVE-2023-49691</a>	Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a>
SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2): All versions affected by <a href="#">CVE-2023-44318</a>	Currently no fix is planned
SCALANCE M874-2 (6GK5874-2AA00-2AA2):	See below
SCALANCE M874-2 (6GK5874-2AA00-2AA2): All versions < V8.0 affected by <a href="#">CVE-2022-46143</a> , <a href="#">CVE-2023-44319</a> , <a href="#">CVE-2023-44322</a> , <a href="#">CVE-2023-44373</a> , <a href="#">CVE-2023-44374</a> , <a href="#">CVE-2023-49691</a>	Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a>

<p>SCALANCE M874-2 (6GK5874-2AA00-2AA2): All versions affected by <a href="#">CVE-2023-44318</a></p>	Currently no fix is planned
<p>SCALANCE M874-3 (6GK5874-3AA00-2AA2):</p>	See below
<p>SCALANCE M874-3 (6GK5874-3AA00-2AA2): All versions &lt; V8.0 affected by <a href="#">CVE-2022-46143</a>, <a href="#">CVE-2023-44319</a>, <a href="#">CVE-2023-44322</a>, <a href="#">CVE-2023-44373</a>, <a href="#">CVE-2023-44374</a>, <a href="#">CVE-2023-49691</a></p>	Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a>
<p>SCALANCE M874-3 (6GK5874-3AA00-2AA2): All versions affected by <a href="#">CVE-2023-44318</a></p>	Currently no fix is planned
<p>SCALANCE M876-3 (6GK5876-3AA02-2BA2):</p>	See below
<p>SCALANCE M876-3 (6GK5876-3AA02-2BA2): All versions &lt; V8.0 affected by <a href="#">CVE-2022-46143</a>, <a href="#">CVE-2023-44319</a>, <a href="#">CVE-2023-44322</a>, <a href="#">CVE-2023-44373</a>, <a href="#">CVE-2023-49691</a></p>	Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a>
<p>SCALANCE M876-3 (6GK5876-3AA02-2BA2): All versions affected by <a href="#">CVE-2023-44318</a></p>	Currently no fix is planned
<p>SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2):</p>	See below
<p>SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2): All versions &lt; V8.0 affected by <a href="#">CVE-2022-46143</a>, <a href="#">CVE-2023-44319</a>, <a href="#">CVE-2023-44322</a>, <a href="#">CVE-2023-44373</a>, <a href="#">CVE-2023-44374</a>, <a href="#">CVE-2023-49691</a></p>	Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a>
<p>SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2): All versions affected by <a href="#">CVE-2023-44318</a></p>	Currently no fix is planned
<p>SCALANCE M876-4 (6GK5876-4AA10-2BA2):</p>	See below

<p>SCALANCE M876-4 (6GK5876-4AA10-2BA2):</p> <p>All versions &lt; V8.0 affected by <a href="#">CVE-2022-46143</a>, <a href="#">CVE-2023-44319</a>, <a href="#">CVE-2023-44322</a>, <a href="#">CVE-2023-44373</a>, <a href="#">CVE-2023-44374</a>, <a href="#">CVE-2023-49691</a></p>	<p>Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a></p>
<p>SCALANCE M876-4 (6GK5876-4AA10-2BA2):</p> <p>All versions affected by <a href="#">CVE-2023-44318</a></p>	<p>Currently no fix is planned</p>
<p>SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2):</p>	<p>See below</p>
<p>SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2):</p> <p>All versions &lt; V8.0 affected by <a href="#">CVE-2022-46143</a>, <a href="#">CVE-2023-44319</a>, <a href="#">CVE-2023-44322</a>, <a href="#">CVE-2023-44373</a>, <a href="#">CVE-2023-44374</a>, <a href="#">CVE-2023-49691</a></p>	<p>Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a></p>
<p>SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2):</p> <p>All versions affected by <a href="#">CVE-2023-44318</a></p>	<p>Currently no fix is planned</p>
<p>SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2):</p>	<p>See below</p>
<p>SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2):</p> <p>All versions &lt; V8.0 affected by <a href="#">CVE-2022-46143</a>, <a href="#">CVE-2023-44319</a>, <a href="#">CVE-2023-44322</a>, <a href="#">CVE-2023-44373</a>, <a href="#">CVE-2023-44374</a>, <a href="#">CVE-2023-49691</a></p>	<p>Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a></p>
<p>SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2):</p> <p>All versions affected by <a href="#">CVE-2023-44318</a></p>	<p>Currently no fix is planned</p>
<p>SCALANCE MUM-800 family:</p>	<p>See below</p>
<p>SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1):</p>	<p>See below</p>
<p>SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1):</p> <p>All versions &lt; V8.0 affected by <a href="#">CVE-2022-46143</a>, <a href="#">CVE-2023-44319</a>, <a href="#">CVE-2023-44322</a>, <a href="#">CVE-2023-44373</a>, <a href="#">CVE-2023-44374</a>, <a href="#">CVE-2023-49691</a></p>	<p>Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a></p>

SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1): All versions affected by <a href="#">CVE-2023-44318</a>	Currently no fix is planned
SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1):	See below
SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1): All versions < V8.0 affected by <a href="#">CVE-2022-46143</a> , <a href="#">CVE-2023-44319</a> , <a href="#">CVE-2023-44322</a> , <a href="#">CVE-2023-44373</a> , <a href="#">CVE-2023-44374</a> , <a href="#">CVE-2023-49691</a>	Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a>
SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1): All versions affected by <a href="#">CVE-2023-44318</a>	Currently no fix is planned
SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1):	See below
SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1): All versions < V8.0 affected by <a href="#">CVE-2022-46143</a> , <a href="#">CVE-2023-44319</a> , <a href="#">CVE-2023-44322</a> , <a href="#">CVE-2023-44373</a> , <a href="#">CVE-2023-44374</a> , <a href="#">CVE-2023-49691</a>	Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a>
SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1): All versions affected by <a href="#">CVE-2023-44318</a>	Currently no fix is planned
SCALANCE S615 family:	See below
SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2):	See below
SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2): All versions < V8.0 affected by <a href="#">CVE-2022-46143</a> , <a href="#">CVE-2023-44319</a> , <a href="#">CVE-2023-44322</a> , <a href="#">CVE-2023-44373</a> , <a href="#">CVE-2023-44374</a> , <a href="#">CVE-2023-49691</a>	Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a>
SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2): All versions affected by <a href="#">CVE-2023-44318</a>	Currently no fix is planned
SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2):	See below

<p>SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2): All versions &lt; V8.0 affected by <a href="#">CVE-2022-46143</a>, <a href="#">CVE-2023-44319</a>, <a href="#">CVE-2023-44322</a>, <a href="#">CVE-2023-44373</a>, <a href="#">CVE-2023-44374</a>, <a href="#">CVE-2023-49691</a></p>	<p>Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826372/">https://support.industry.siemens.com/cs/ww/en/view/109826372/</a></p>
<p>SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2): All versions affected by <a href="#">CVE-2023-44318</a></p>	<p>Currently no fix is planned</p>

## **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-2022-46143**

Affected devices do not check the TFTP blocksize correctly. This could allow an authenticated attacker to read from an uninitialized buffer that potentially contains previously allocated data.

CVSS v3.1 Base Score      2.7  
CVSS Vector                [CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C](#)  
CWE                            CWE-1284: Improper Validation of Specified Quantity in Input

### **Vulnerability CVE-2023-44318**

Affected devices use a hardcoded key to obfuscate the configuration backup that an administrator can export from the device. This could allow an authenticated attacker with administrative privileges or an attacker that obtains a configuration backup to extract configuration information from the exported file.

CVSS v3.1 Base Score      4.9  
CVSS Vector                [CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:U/RC:C](#)  
CWE                            CWE-321: Use of Hard-coded Cryptographic Key

**Vulnerability CVE-2023-44319**

Affected devices use a weak checksum algorithm to protect the configuration backup that an administrator can export from the device. This could allow an authenticated attacker with administrative privileges or an attacker that tricks a legitimate administrator to upload a modified configuration file to change the configuration of an affected device.

CVSS v3.1 Base Score 4.9  
CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C](#)  
CWE CWE-328: Use of Weak Hash

**Vulnerability CVE-2023-44322**

Affected devices can be configured to send emails when certain events occur on the device. When presented with an invalid response from the SMTP server, the device triggers an error that disrupts email sending. An attacker with access to the network can use this to do disable notification of users when certain events occur.

CVSS v3.1 Base Score 3.7  
CVSS Vector [CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C](#)  
CWE CWE-252: Unchecked Return Value

**Vulnerability CVE-2023-44373**

Affected devices do not properly sanitize an input field. This could allow an authenticated remote attacker with administrative privileges to inject code or spawn a system root shell. Follow-up of CVE-2022-36323.

CVSS v3.1 Base Score 9.1  
CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C](#)  
CVSS v4.0 Base Score 9.4  
CVSS Vector [CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H](#)  
CWE CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

**Vulnerability CVE-2023-44374**

Affected devices allow to change the password, but insufficiently check which password is to be changed. With this an authenticated attacker could, under certain conditions, be able to change the password of another, potential admin user allowing her to escalate her privileges.

CVSS v3.1 Base Score 6.5  
CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C](#)  
CWE CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context

**Vulnerability CVE-2023-49691**

An Improper Neutralization of Special Elements used in an OS Command with root privileges vulnerability exists in the handling of the DDNS configuration. This could allow malicious local administrators to issue commands on system level after a successful IP address update.

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): Moved CVE-2023-44321 to SSA-087301 as fixed in V8.1, moved CVE-2023-44320 to SSA-068047 as fixed in V7.2.2

## **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](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.