Siemens Security Advisory by Siemens ProductCERT

SSA-710008: Multiple Web Vulnerabilities in SCALANCE Products

Publication Date:	2022-08-09
Last Update:	2026-04-14
Current Version:	V1.5
CVSS v3.1 Base Score:	9.1

▼ SUMMARY

SCALANCE devices contain multiple vulnerabilities in MSPS based product lines that could allow authenticated remote attackers to execute custom code or create a XSS situation, as well as unauthenticated remote attackers to create a denial of service condition.

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

▼ KNOWN AFFECTED PRODUCTS

Un-/Collapse All

Affected Product and Versions	Remediation
SCALANCE M-800 family (incl. S615, MUM-800 and RM1224)	Show more details
SCALANCE SC-600 family	Show more details
SCALANCE W-700 IEEE 802.11ax family	Show more details
SCALANCE W-700 IEEE 802.11n family	Show more details
SCALANCE W-1700 IEEE 802.11ac family	Show more details
SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG family	Show more details
SCALANCE XM-400/XR-500 family	Show more details

▼ MITIGATIONS

Siemens has identified the following specific mitigations that customers can apply to reduce the risk:

- Apply the principle of least privileges for accounts configured on the affected devices
- Restrict network access in affected system(s) to ports 80/TCP and 443/TCP to trusted IP addresses and personal only

Product-specific remediations or mitigations can be found in the section Known Affected Products.
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

VULNERABILITY DESCRIPTION

Un-/Collapse All

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-2022-36323

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.

CVSS v3.1 Base Score	9.1
CVSS v3.1 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
CWE	CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

Vulnerability CVE-2022-36324

Affected devices do not properly handle the renegotiation of SSL/TLS parameters. This could allow an unauthenticated remote attacker to bypass the TCP brute force prevention and lead to a denial of service condition for the duration of the attack.

CVSS v3.1 Base Score	7.5
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-770: Allocation of Resources Without Limits or Throttling

Vulnerability CVE-2022-36325

Affected devices do not properly sanitize data introduced by an user when rendering the web interface. This could allow an authenticated remote attacker with administrative privileges to inject code and lead to a DOM-based XSS.

CVSS v3.1 Base Score	6.8
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

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	(2022-08-09):	Publication Date
V1.1	(2022-09-13):	Added fix for SCALANCE M-800, SCALANCE MUM-800 and RUGGEDCOM RM1224 families, as well as for SCALANCE S615

		families; All affected product families were expanded
V1.2	(2023-01-10):	Added fix for SCALANCE W-700 IEEE 802.11ax product family
V1.3	(2023-04-11):	Added fix for SCALANCE XM-400/XR-500 family and for SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG family
V1.4	(2023-10-10):	Added that SCALANCE SC-600 family was also affected by CVE-2022-36324
V1.5	(2026-04-14):	Added fix for SCALANCE W-700 IEEE 802.11n family

▼ TERMS OF USE