Siemens Security Advisory by Siemens ProductCERT

SSA-552702: Privilege Escalation Vulnerability in the Web Interface of SCALANCE and RUGGEDCOM Products

Publication Date:	2022-10-11
Last Update:	2026-04-14
Current Version:	V1.6
CVSS v3.1 Base Score:	8.8

▼ SUMMARY

The products listed below do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.

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:

- Use ACLs to restrict access to the device web server
- Restrict access to the device web server ports (default 443/tcp or 80/tcp) to trusted networks and client IP addresses

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-2022-31765

Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.

CVSS v3.1 Base Score	8.8
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-862: Missing Authorization

▼ 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	(2022-11-08):	Added missing affected product SCALANCE S615
V1.2	(2022-12-13):	Added fix for SCALANCE SC-600 family
V1.3	(2023-01-10):	Added fix for SCALANCE W-700 IEEE 802.11ax product family
V1.4	(2023-03-14):	Added missing affected products SCALANCE S615 EEC (6GK5615-0AA01-2AA2) and SCALANCE M876-4 (6GK5876-4AA10-2BA2)
V1.5	(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
V1.6	(2026-04-14):	Added fix for SCALANCE W-700 IEEE 802.11n family

▼ TERMS OF USE