SSA-723487: RADIUS Protocol Susceptible to Forgery Attacks (CVE-2024-3596) - Impact to SCALANCE, RUGGEDCOM and Related Products

Publication Date: 2024-07-09
Last Update: 2025-07-08
Current Version: V1.7
CVSS v3.1 Base Score: 9.0
CVSS v4.0 Base Score: 9.1

SUMMARY

This advisory documents the impact of CVE-2024-3596 (also dubbed “Blastradius"), a vulnerability in the RADIUS protocol, to SCALANCE, RUGGEDCOM and related products.

The vulnerability could allow on-path attackers, located between a Network Access Server (the RADIUS client, e.g., SCALANCE or RUGGEDCOM devices) and a RADIUS server (e.g., SINEC INS), to forge Access-Request packets in a way that enables them to modify the corresponding server response packet at will, e.g., turning an “Access-Reject” message into an “Access-Accept”. This would cause the Network Access Server to grant the attackers access to the network with the attackers desired authorization (and without the need of knowing or guessing legitimate access credentials).

Further details incl. external references can be found in the chapter “Additional Information”. Siemens has released new versions for several affected products and recommends to update to the latest versions, and to configure the updated systems as recommended in the chapter “Additional Information”. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available. See chapter “Additional Information” for details.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM CROSSBOW: All versions < V5.6 affected by CVE-2024-3596	Update to V5.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109976555/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS V4.X family:	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See recommendations from section Workarounds and Mitigations
RUGGEDCOM i800: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM ROS V4.X NC products:	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See recommendations from section Workarounds and Mitigations
RUGGEDCOM i800NC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM i801NC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM i802NC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM i803NC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM M2100NC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM M2200NC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM M969NC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RMC30NC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC8388NC V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RP110NC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600FNC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600NC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600TNC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS400NC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS401NC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS416NC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416NCv2 V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416PNC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416PNCv2 V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000ANC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000HNC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000NC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000TNC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS900GNC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GNC(32M) V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GPNC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900LNC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900MNC-GETS-C01: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900MNC-GETS-XX: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900MNC-STND-XX: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900MNC-STND-XX-C01: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS900NC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900NC(32M) V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS910LNC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS910NC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS920LNC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS930LNC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS940GNC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS969NC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RSG2100NC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100NC(32M) V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100PNC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100PNC (32M) V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2200NC: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2288NC V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300NC V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300PNC V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RSG2488NC V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920PNC V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM i801: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM i802: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM i803: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM M2100: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM M2200: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM M969: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RMC30: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC8388 V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RP110: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600F: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600T: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS400: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS401: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS416: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416P: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416Pv2 V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416v2 V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000A: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000H: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000T: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS900: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900 (32M) V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900G: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900G (32M) V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GP: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900L: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900M-GETS-C01: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900M-GETS-XX: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS900M-STND-C01: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900M-STND-XX: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900W: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS910: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS910L: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS910W: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS920L: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS920W: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS930L: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS930W: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS940G: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS969: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100 (32M) V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100P: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100P (32M) V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RSG2200: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2288 V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300 V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300P V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488 V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920P V4.X: All versions < V4.3.11 affected by CVE-2024-3596	Update to V4.3.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109977251/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS V5.X family:	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC8388 V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM ROS V5.X NC products:	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC8388NC V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416NCv2 V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416PNCv2 V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GNC(32M) V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900NC(32M) V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100NC(32M) V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100PNC (32M) V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RSG2288NC V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300NC V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300PNC V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488NC V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920PNC V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSL910NC: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416Pv2 V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416v2 V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS900 (32M) V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900G (32M) V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100 (32M) V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100P (32M) V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2288 V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300 V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300P V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488 V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RSG907R: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG908C: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG909R: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG910C: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920P V5.X: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSL910: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RST2228: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RST2228P: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RST916C: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RST916P: All versions < V5.10.0 affected by CVE-2024-3596	Update to V5.10.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989952/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX II family:	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX MX5000: All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX MX5000RE: All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1400: All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1500: All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1501: All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1510: All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1511: All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1512: All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations

RUGGEDCOM ROX RX1524: All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1536: All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX5000: All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RST2428P (6GK6242-6PA00): All versions < V3.2 affected by CVE-2024-3596	Update to V3.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109988839/ See further recommendations from section Workarounds and Mitigations
SCALANCE M-800 family (incl. S615, MUM-800 and RM1224):	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See recommendations from section Workarounds and Mitigations
RUGGEDCOM RM1224 family (6GK6108-4AM00):	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See recommendations from section Workarounds and Mitigations
RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE M-800 family:	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See recommendations from section Workarounds and Mitigations

SCALANCE M804PB (6GK5804-0AP00-2AA2): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE M812-1 ADSL-Router family:	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See recommendations from section Workarounds and Mitigations
SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE M816-1 ADSL-Router family:	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See recommendations from section Workarounds and Mitigations
SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations

SCALANCE M874-2 (6GK5874-2AA00-2AA2): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE M874-3 (6GK5874-3AA00-2AA2): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE M876-3 (6GK5876-3AA02-2BA2): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE M876-4 (6GK5876-4AA10-2BA2): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations

SCALANCE MUM-800 family:	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See recommendations from section Workarounds and Mitigations
SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations

SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE S615 family:	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See recommendations from section Workarounds and Mitigations
SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2): All versions < V8.2 affected by CVE-2024-3596	Update to V8.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109976047/ See further recommendations from section Workarounds and Mitigations
SCALANCE SC-600 family:	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE SC622-2C (6GK5622-2GS00-2AC2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE SC626-2C (6GK5626-2GS00-2AC2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE SC632-2C (6GK5632-2GS00-2AC2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE SC636-2C (6GK5636-2GS00-2AC2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE SC642-2C (6GK5642-2GS00-2AC2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE SC646-2C (6GK5646-2GS00-2AC2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W-700 IEEE 802.11ax family:	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See recommendations from section Workarounds and Mitigations
SCALANCE WAB762-1 (6GK5762-1AJ00-6AA0): All versions < V3.0.0 affected by CVE-2024-3596	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See further recommendations from section Workarounds and Mitigations
SCALANCE WAM763-1 (6GK5763-1AL00-7DA0): All versions < V3.0.0 affected by CVE-2024-3596	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See further recommendations from section Workarounds and Mitigations
SCALANCE WAM763-1 (ME) (6GK5763-1AL00-7DC0): All versions < V3.0.0 affected by CVE-2024-3596	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See further recommendations from section Workarounds and Mitigations
SCALANCE WAM763-1 (US) (6GK5763-1AL00-7DB0): All versions < V3.0.0 affected by CVE-2024-3596	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See further recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 (6GK5766-1GE00-7DA0): All versions < V3.0.0 affected by CVE-2024-3596	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See further recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 (ME) (6GK5766-1GE00-7DC0): All versions < V3.0.0 affected by CVE-2024-3596	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See further recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 (US) (6GK5766-1GE00-7DB0): All versions < V3.0.0 affected by CVE-2024-3596	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See further recommendations from section Workarounds and Mitigations

SCALANCE WAM766-1 EEC (6GK5766-1GE00-7TA0): All versions < V3.0.0 affected by CVE-2024-3596	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See further recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 EEC (ME) (6GK5766-1GE00-7TC0): All versions < V3.0.0 affected by CVE-2024-3596	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See further recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 EEC (US) (6GK5766-1GE00-7TB0): All versions < V3.0.0 affected by CVE-2024-3596	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See further recommendations from section Workarounds and Mitigations
SCALANCE WUB762-1 (6GK5762-1AJ00-1AA0): All versions < V3.0.0 affected by CVE-2024-3596	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See further recommendations from section Workarounds and Mitigations
SCALANCE WUB762-1 iFeatures (6GK5762-1AJ00-2AA0): All versions < V3.0.0 affected by CVE-2024-3596	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See further recommendations from section Workarounds and Mitigations
SCALANCE WUM763-1 (6GK5763-1AL00-3AA0): All versions < V3.0.0 affected by CVE-2024-3596	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See further recommendations from section Workarounds and Mitigations
SCALANCE WUM763-1 (6GK5763-1AL00-3DA0): All versions < V3.0.0 affected by CVE-2024-3596	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See further recommendations from section Workarounds and Mitigations
SCALANCE WUM763-1 (US) (6GK5763-1AL00-3AB0): All versions < V3.0.0 affected by CVE-2024-3596	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See further recommendations from section Workarounds and Mitigations

SCALANCE WUM763-1 (US) (6GK5763-1AL00-3DB0): All versions < V3.0.0 affected by CVE-2024-3596	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See further recommendations from section Workarounds and Mitigations
SCALANCE WUM766-1 (6GK5766-1GE00-3DA0): All versions < V3.0.0 affected by CVE-2024-3596	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See further recommendations from section Workarounds and Mitigations
SCALANCE WUM766-1 (ME) (6GK5766-1GE00-3DC0): All versions < V3.0.0 affected by CVE-2024-3596	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See further recommendations from section Workarounds and Mitigations
SCALANCE WUM766-1 (USA) (6GK5766-1GE00-3DB0): All versions < V3.0.0 affected by CVE-2024-3596	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109977720/ See further recommendations from section Workarounds and Mitigations
SCALANCE W-700 IEEE 802.11n family:	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AC0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA6): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W734-1 RJ45 (USA) (6GK5734-1FX00-0AB6): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W738-1 M12 (6GK5738-1GY00-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W738-1 M12 (6GK5738-1GY00-0AB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W748-1 M12 (6GK5748-1GD00-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W748-1 M12 (6GK5748-1GD00-0AB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA6): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AC0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (USA) (6GK5774-1FX00-0AB6): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W778-1 M12 (6GK5778-1GY00-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W778-1 M12 (6GK5778-1GY00-0AB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W778-1 M12 EEC (6GK5778-1GY00-0TA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W778-1 M12 EEC (USA) (6GK5778-1GY00-0TB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AC0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 SFP (6GK5786-2FE00-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 SFP (6GK5786-2FE00-0AB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W788-1 M12 (6GK5788-1GD00-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W788-1 M12 (6GK5788-1GD00-0AB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE W788-2 M12 (6GK5788-2GD00-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 (6GK5788-2GD00-0AB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TC0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AB0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AC0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W-1700 IEEE 802.11ac family:	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W1748-1 M12 (6GK5748-1GY01-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W1748-1 M12 (6GK5748-1GY01-0TA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W1788-1 M12 (6GK5788-1GY01-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE W1788-2 EEC M12 (6GK5788-2GY01-0TA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W1788-2 M12 (6GK5788-2GY01-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W1788-2IA M12 (6GK5788-2HY01-0AA0): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE X-300 family (incl. X408 and SIPLUS NET variants):	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See recommendations from section Workarounds and Mitigations
SCALANCE X-300 EEC family:	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (230V, coated) (6GK5302-7GD00-3GA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (230V) (6GK5302-7GD00-3EA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (24V, coated) (6GK5302-7GD00-1GA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (24V) (6GK5302-7GD00-1EA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations

SCALANCE X302-7 EEC (2x 230V, coated) (6GK5302-7GD00-4GA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (2x 230V) (6GK5302-7GD00-4EA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (2x 24V, coated) (6GK5302-7GD00-2GA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (2x 24V) (6GK5302-7GD00-2EA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (230V, coated) (6GK5307-2FD00-3GA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (230V) (6GK5307-2FD00-3EA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (24V, coated) (6GK5307-2FD00-1GA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (24V) (6GK5307-2FD00-1EA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations

SCALANCE X307-2 EEC (2x 230V, coated) (6GK5307-2FD00-4GA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (2x 230V) (6GK5307-2FD00-4EA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (2x 24V, coated) (6GK5307-2FD00-2GA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (2x 24V) (6GK5307-2FD00-2EA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X-300 family:	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See recommendations from section Workarounds and Mitigations
SCALANCE X304-2FE (6GK5304-2BD00-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X306-1LD FE (6GK5306-1BF00-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X320-1 FE (6GK5320-1BD00-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations

SCALANCE X320-1-2LD FE (6GK5320-3BF00-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X300 family:	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See recommendations from section Workarounds and Mitigations
SCALANCE X307-3 (6GK5307-3BL00-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-3LD (6GK5307-3BM00-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2 (6GK5308-2FL00-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LD (6GK5308-2FM00-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH (6GK5308-2FN00-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH+ (6GK5308-2FP00-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations

SCALANCE X310 (6GK5310-0FA00-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X310FE (6GK5310-0BA00-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X-300 RD family:	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See recommendations from section Workarounds and Mitigations
SCALANCE X307-3 (6GK5307-3BL10-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-3LD (6GK5307-3BM10-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2 RD (inkl. SIPLUS variants):	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See recommendations from section Workarounds and Mitigations
SCALANCE X308-2 (6GK5308-2FL10-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SIPLUS NET SCALANCE X308-2 (6AG1308-2FL10-4AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations

SCALANCE X308-2LD (6GK5308-2FM10-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH (6GK5308-2FN10-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH+ (6GK5308-2FP10-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X310 (6GK5310-0FA10-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X310FE (6GK5310-0BA10-2AA3): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M family:	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See recommendations from section Workarounds and Mitigations
SCALANCE X308-2M (6GK5308-2GG00-2AA2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M PoE (6GK5308-2QG00-2AA2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations

SCALANCE X308-2M TS (6GK5308-2GG00-2CA2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M RD family:	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See recommendations from section Workarounds and Mitigations
SCALANCE X308-2M (6GK5308-2GG10-2AA2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M PoE (6GK5308-2QG10-2AA2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M TS (6GK5308-2GG10-2CA2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X408 family:	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE X408-2 (6GK5408-2FD00-2AA2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR-300 (6GK5324-xGGxx) family:	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See recommendations from section Workarounds and Mitigations

SCALANCE XR324-12M (230V, ports on front) (6GK5324-0GG00-3AR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (230V, ports on rear) (6GK5324-0GG00-3HR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (24V, ports on front) (6GK5324-0GG00-1AR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (24V, ports on rear) (6GK5324-0GG00-1HR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M TS (24V) (6GK5324-0GG00-1CR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR-300 RD family:	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (230V, ports on front) (6GK5324-0GG10-3AR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (230V, ports on rear) (6GK5324-0GG10-3HR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR324-12M (24V, ports on front) (6GK5324-0GG10-1AR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (24V, ports on rear) (6GK5324-0GG10-1HR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M TS (24V) (6GK5324-0GG10-1CR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR-300 EEC family:	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front) (6GK5324-4GG00-3ER2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG00-3JR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (24V, ports on front) (6GK5324-4GG00-1ER2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (24V, ports on rear) (6GK5324-4GG00-1JR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front) (6GK5324-4GG00-4ER2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG00-4JR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 24V, ports on front) (6GK5324-4GG00-2ER2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 24V, ports on rear) (6GK5324-4GG00-2JR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR-300 EEC RD family:	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front) (6GK5324-4GG10-3ER2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG10-3JR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (24V, ports on front) (6GK5324-4GG10-1ER2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR324-4M EEC (24V, ports on rear) (6GK5324-4GG10-1JR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front) (6GK5324-4GG10-4ER2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG10-4JR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 24V, ports on front) (6GK5324-4GG10-2ER2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 24V, ports on rear) (6GK5324-4GG10-2JR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR-300 POE family:	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE (230V, ports on front) (6GK5324-4QG00-3AR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE (230V, ports on rear) (6GK5324-4QG00-3HR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR324-4M PoE (24V, ports on front) (6GK5324-4QG00-1AR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE (24V, ports on rear) (6GK5324-4QG00-1HR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE TS (24V, ports on front) (6GK5324-4QG00-1CR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR-300 POE RD family:	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE (230V, ports on front) (6GK5324-4QG10-3AR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE (230V, ports on rear) (6GK5324-4QG10-3HR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE (24V, ports on front) (6GK5324-4QG10-1AR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE (24V, ports on rear) (6GK5324-4QG10-1HR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR324-4M PoE TS (24V, ports on front) (6GK5324-4QG10-1CR2): All versions < V4.1.9 affected by CVE-2024-3596	Update to V4.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109982245/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG family:	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See recommendations from section Workarounds and Mitigations
SCALANCE XB-200 family:	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See recommendations from section Workarounds and Mitigations
SCALANCE XB205-3 (SC, PN) (6GK5205-3BB00-2AB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB205-3 (ST, E/IP) (6GK5205-3BD00-2TB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB205-3 (ST, E/IP) (6GK5205-3BB00-2TB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB205-3 (ST, PN) (6GK5205-3BD00-2AB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB205-3LD (SC, E/IP) (6GK5205-3BF00-2TB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations

SCALANCE XB205-3LD (SC, PN) (6GK5205-3BF00-2AB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB206-2 (SC) (6GK5206-2BD00-2TB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB206-2 (ST/BFOC) (6GK5206-2BF00-2TB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB206-2 LD (6GK5206-2BF00-2AB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB206-2 SC (6GK5206-2BD00-2AB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB206-2 ST (6GK5206-2BB00-2AB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB206-2LD (6GK5206-2BB00-2TB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB208 (E/IP) (6GK5208-0BA00-2TB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations

SCALANCE XB208 (PN) (6GK5208-0BA00-2AB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB213-3 (SC, E/IP) (6GK5213-3BD00-2TB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB213-3 (SC, PN) (6GK5213-3BD00-2AB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB213-3 (ST, E/IP) (6GK5213-3BB00-2TB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB213-3 (ST, PN) (6GK5213-3BB00-2AB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB213-3LD (SC, E/IP) (6GK5213-3BF00-2TB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB213-3LD (SC, PN) (6GK5213-3BF00-2AB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB216 (E/IP) (6GK5216-0BA00-2TB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations

SCALANCE XB216 (PN) (6GK5216-0BA00-2AB2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC-200 family:	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See recommendations from section Workarounds and Mitigations
SCALANCE XC206-2 (SC) (6GK5206-2BD00-2AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC206-2 (ST/BFOC) (6GK5206-2BB00-2AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC206-2G PoE (6GK5206-2RS00-2AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC206-2G PoE (54 V DC) (6GK5206-2RS00-5AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC206-2G PoE EEC (54 V DC) (6GK5206-2RS00-5FC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC206-2SFP (6GK5206-2BS00-2AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations

SCALANCE XC206-2SFP EEC (6GK5206-2BS00-2FC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC206-2SFP G (6GK5206-2GS00-2AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC206-2SFP G (EIP DEF.) (6GK5206-2GS00-2TC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC206-2SFP G EEC (6GK5206-2GS00-2FC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC208 (6GK5208-0BA00-2AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC208EEC (6GK5208-0BA00-2FC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC208G (6GK5208-0GA00-2AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC208G (EIP def.) (6GK5208-0GA00-2TC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations

SCALANCE XC208G EEC (6GK5208-0GA00-2FC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC208G PoE (6GK5208-0RA00-2AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC208G PoE (54 V DC) (6GK5208-0RA00-5AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC216 (6GK5216-0BA00-2AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC216-3G PoE (6GK5216-3RS00-2AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC216-3G PoE (54 V DC) (6GK5216-3RS00-5AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC216-4C (6GK5216-4BS00-2AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC216-4C G (6GK5216-4GS00-2AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations

SCALANCE XC216-4C G (EIP Def.) (6GK5216-4GS00-2TC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC216-4C G EEC (6GK5216-4GS00-2FC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC216EEC (6GK5216-0BA00-2FC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC224 (6GK5224-0BA00-2AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC224-4C G (6GK5224-4GS00-2AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC224-4C G (EIP Def.) (6GK5224-4GS00-2TC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC224-4C G EEC (6GK5224-4GS00-2FC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SIPLUS NET SCALANCE XC206-2 (6AG1206-2BB00-7AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations

SIPLUS NET SCALANCE XC206-2SFP (6AG1206-2BS00-7AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SIPLUS NET SCALANCE XC208 (6AG1208-0BA00-7AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SIPLUS NET SCALANCE XC216-4C (6AG1216-4BS00-7AC2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XF-200BA family:	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See recommendations from section Workarounds and Mitigations
SCALANCE XF204 (6GK5204-0BA00-2GF2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XF204 DNA (6GK5204-0BA00-2YF2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XF204-2BA (6GK5204-2AA00-2GF2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XF204-2BA DNA (6GK5204-2AA00-2YF2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations

SCALANCE XF204G (6GK5204-0GA00-1UF2): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP-200 family:	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See recommendations from section Workarounds and Mitigations
SCALANCE XP208 (6GK5208-0HA00-2AS6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP208 (6GK5208-0HA10-2AS6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP208 (Ethernet/IP) (6GK5208-0HA00-2TS6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP208EEC (6GK5208-0HA00-2ES6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP208EEC (6GK5208-0HA10-2ES6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP208G (6GK5208-0XA00-2AS6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations

SCALANCE XP208G EEC (6GK5208-0XA00-2ES6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP208G PoE EEC (6GK5208-0YA00-5ES6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP208G PP (6GK5208-0JA00-2AS6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP208PoE EEC (6GK5208-0UA00-5ES6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP208PoE EEC (6GK5208-0UA10-5ES6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP216 (6GK5216-0HA00-2AS6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP216 (Ethernet/IP) (6GK5216-0HA00-2TS6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP216 (V2) (6GK5216-0HA10-2AS6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations

SCALANCE XP216EEC (6GK5216-0HA00-2ES6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP216EEC (V2) (6GK5216-0HA10-2ES6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP216G (6GK5216-0XA00-2AS6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP216G EEC (6GK5216-0XA00-2ES6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP216G PoE EEC (6GK5216-0YA00-5ES6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP216POE EEC (6GK5216-0UA00-5ES6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP216PoE EEC (V2) (6GK5216-0UA10-5ES6): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR-300WG family:	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See recommendations from section Workarounds and Mitigations

SCALANCE XR324WG (24 x FE, AC 230V) (6GK5324-0BA00-3AR3): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324WG (24 X FE, DC 24V) (6GK5324-0BA00-2AR3): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR326-2C PoE WG (6GK5326-2QS00-3AR3): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR326-2C PoE WG (without UL) (6GK5326-2QS00-3RR3): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR328-4C WG (24XFE, 4XGE, 24V) (6GK5328-4FS00-2AR3): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR328-4C WG (24xFE, 4xGE,DC24V) (6GK5328-4FS00-2RR3): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR328-4C WG (24xFE,4xGE,AC230V) (6GK5328-4FS00-3AR3): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR328-4C WG (24xFE,4xGE,AC230V) (6GK5328-4FS00-3RR3): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR328-4C WG (28xGE, AC 230V) (6GK5328-4SS00-3AR3): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR328-4C WG (28xGE, DC 24V) (6GK5328-4SS00-2AR3): All versions < V4.6 affected by CVE-2024-3596	Update to V4.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109977185/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 family:	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See recommendations from section Workarounds and Mitigations
SCALANCE XC-300 family:	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See recommendations from section Workarounds and Mitigations
SCALANCE XC316-8 (6GK5324-8TS00-2AC2): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC324-4 (6GK5328-4TS00-2AC2): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC324-4 EEC (6GK5328-4TS00-2EC2): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC332 (6GK5332-0GA00-2AC2): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations

SCALANCE XC-400 family:	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See recommendations from section Workarounds and Mitigations
SCALANCE XC416-8 (6GK5424-8TR00-2AC2): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC424-4 (6GK5428-4TR00-2AC2): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC432 (6GK5432-0GR00-2AC2): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR-300 (6GK5334-xTSxx) family:	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See recommendations from section Workarounds and Mitigations
SCALANCE XR302-32 (6GK5334-5TS00-2AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR302-32 (6GK5334-5TS00-3AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR302-32 (6GK5334-5TS00-4AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR322-12 (6GK5334-3TS00-2AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR322-12 (6GK5334-3TS00-3AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR322-12 (6GK5334-3TS00-4AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR326-8 (6GK5334-2TS00-2AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR326-8 (6GK5334-2TS00-3AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR326-8 (6GK5334-2TS00-4AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR326-8 EEC (6GK5334-2TS00-2ER3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR-500 (6GK5334-xTSxx) family:	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See recommendations from section Workarounds and Mitigations

SCALANCE XR502-32 (6GK5534-5TR00-2AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR502-32 (6GK5534-5TR00-3AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR502-32 (6GK5534-5TR00-4AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR522-12 (6GK5534-3TR00-2AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR522-12 (6GK5534-3TR00-3AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR522-12 (6GK5534-3TR00-4AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR526-8 (6GK5534-2TR00-2AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR526-8 (6GK5534-2TR00-3AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR526-8 (6GK5534-2TR00-4AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR-500WG family:	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See recommendations from section Workarounds and Mitigations
SCALANCE XR524-8WG (6GK5532-2SR00-2AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR524-8WG (6GK5532-2SR00-2RR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR524-8WG (6GK5532-2SR00-3AR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR524-8WG (6GK5532-2SR00-3RR3): All versions < V1.3 affected by CVE-2024-3596	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109977441/ See further recommendations from section Workarounds and Mitigations
SCALANCE XCM-/XRM-/XCH-/XRH-300 family:	Update to V3.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109988839/ See recommendations from section Workarounds and Mitigations
SCALANCE XCH328 (6GK5328-4TS01-2EC2): All versions < V3.2 affected by CVE-2024-3596	Update to V3.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109988839/ See further recommendations from section Workarounds and Mitigations

SCALANCE XCM324 (6GK5324-8TS01-2AC2): All versions < V3.2 affected by CVE-2024-3596	Update to V3.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109988839/ See further recommendations from section Workarounds and Mitigations
SCALANCE XCM328 (6GK5328-4TS01-2AC2): All versions < V3.2 affected by CVE-2024-3596	Update to V3.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109988839/ See further recommendations from section Workarounds and Mitigations
SCALANCE XCM332 (6GK5332-0GA01-2AC2): All versions < V3.2 affected by CVE-2024-3596	Update to V3.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109988839/ See further recommendations from section Workarounds and Mitigations
SCALANCE XRH334 (24 V DC, 8xFO, CC) (6GK5334-2TS01-2ER3): All versions < V3.2 affected by CVE-2024-3596	Update to V3.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109988839/ See further recommendations from section Workarounds and Mitigations
SCALANCE XRM334 (230 V AC, 12xFO) (6GK5334-3TS01-3AR3): All versions < V3.2 affected by CVE-2024-3596	Update to V3.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109988839/ See further recommendations from section Workarounds and Mitigations
SCALANCE XRM334 (230 V AC, 8xFO) (6GK5334-2TS01-3AR3): All versions < V3.2 affected by CVE-2024-3596	Update to V3.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109988839/ See further recommendations from section Workarounds and Mitigations
SCALANCE XRM334 (230V AC, 2x10G, 24xSFP, 8xSFP+) (6GK5334-5TS01-3AR3): All versions < V3.2 affected by CVE-2024-3596	Update to V3.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109988839/ See further recommendations from section Workarounds and Mitigations
SCALANCE XRM334 (24 V DC, 12xFO) (6GK5334-3TS01-2AR3): All versions < V3.2 affected by CVE-2024-3596	Update to V3.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109988839/ See further recommendations from section Workarounds and Mitigations

SCALANCE XRM334 (24 V DC, 8xFO) (6GK5334-2TS01-2AR3): All versions < V3.2 affected by CVE-2024-3596	Update to V3.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109988839/ See further recommendations from section Workarounds and Mitigations
SCALANCE XRM334 (24V DC, 2x10G, 24xSFP, 8xSFP+) (6GK5334-5TS01-2AR3): All versions < V3.2 affected by CVE-2024-3596	Update to V3.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109988839/ See further recommendations from section Workarounds and Mitigations
SCALANCE XRM334 (2x230 V AC, 12xFO) (6GK5334-3TS01-4AR3): All versions < V3.2 affected by CVE-2024-3596	Update to V3.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109988839/ See further recommendations from section Workarounds and Mitigations
SCALANCE XRM334 (2x230 V AC, 8xFO) (6GK5334-2TS01-4AR3): All versions < V3.2 affected by CVE-2024-3596	Update to V3.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109988839/ See further recommendations from section Workarounds and Mitigations
SCALANCE XRM334 (2x230V AC, 2x10G, 24xSFP, 8xSFP+) (6GK5334-5TS01-4AR3): All versions < V3.2 affected by CVE-2024-3596	Update to V3.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109988839/ See further recommendations from section Workarounds and Mitigations
SCALANCE XM-400/XR-500 family:	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XM-400 family:	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XM408-4C (6GK5408-4GP00-2AM2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XM408-4C (L3 int.) (6GK5408-4GQ00-2AM2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XM408-8C (6GK5408-8GS00-2AM2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE XM408-8C (L3 int.) (6GK5408-8GR00-2AM2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XM416-4C (6GK5416-4GS00-2AM2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XM416-4C (L3 int.) (6GK5416-4GR00-2AM2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR-500 family:	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR524-8C, 1x230V (6GK5524-8GS00-3AR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR524-8C, 1x230V (L3 int.) (6GK5524-8GR00-3AR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR524-8C, 24V (6GK5524-8GS00-2AR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR524-8C, 24V (L3 int.) (6GK5524-8GR00-2AR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR524-8C, 2x230V (6GK5524-8GS00-4AR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR524-8C, 2x230V (L3 int.) (6GK5524-8GR00-4AR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR526-8C, 1x230V (6GK5526-8GS00-3AR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR526-8C, 1x230V (L3 int.) (6GK5526-8GR00-3AR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE XR526-8C, 24V (6GK5526-8GS00-2AR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR526-8C, 24V (L3 int.) (6GK5526-8GR00-2AR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR526-8C, 2x230V (6GK5526-8GS00-4AR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR526-8C, 2x230V (L3 int.) (6GK5526-8GR00-4AR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR528-6M (6GK5528-0AA00-2AR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR528-6M (2HR2, L3 int.) (6GK5528-0AR00-2HR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR528-6M (2HR2) (6GK5528-0AA00-2HR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR528-6M (L3 int.) (6GK5528-0AR00-2AR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR552-12M (6GK5552-0AA00-2AR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR552-12M (2HR2, L3 int.) (6GK5552-0AR00-2AR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR552-12M (2HR2) (6GK5552-0AA00-2HR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR552-12M (2HR2) (6GK5552-0AR00-2HR2): All versions affected by CVE-2024-3596	Currently no fix is available See recommendations from section Workarounds and Mitigations

SINEC INS: All versions < V1.0 SP2 Update 4 only when the Relay feature is enabled affected by CVE-2024-3596	Update to V1.0 SP2 Update 4 or later version 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:

- Restrict access to the networks where RADIUS messages are exchanged (e.g., send RADIUS traffic via management network or a dedicated VLAN)
- Configure the RADIUS server to require the presence of a Message-Authenticator attribute in all Access-Request packets from RADIUS client devices that support it

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

RUGGEDCOM CROSSBOW is a secure access management solution designed to provide NERC CIP compliant access to Intelligent Electronic Devices.

RUGGEDCOM Ethernet switches are used to operate reliably in electrical harsh and climatically demanding environments such as electric utility substations and traffic control cabinets.

RUGGEDCOM RST2428P is a SINEC OS-based Layer 2 Ethernet switch with up to 28 non-blocking interfaces.

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

SCALANCE SC-600 devices are used to protect trusted industrial networks from untrusted networks. They allow filtering incoming and outgoing network connections in different ways.

SCALANCE W-1700 products are wireless communication devices based on IEEE 802.11ac 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.

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.

SCALANCE X switches are used to connect industrial components like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs).

SINEC INS (Infrastructure Network Services) is a web-based application that combines various network services in one tool. This simplifies installation and administration of all network services relevant for industrial networks.

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-2024-3596

RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by a local attacker who can modify responses Access-Reject or Access-Accept using a chosen-prefix collision attack against MD5 Response Authenticator signature.

CVSS v3.1 Base Score	9.0
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
CVSS v4.0 Base Score	9.1
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:N/SC:H/SI:H/SA:H
CWE	CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel

ADDITIONAL INFORMATION

Note regarding SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 family (MSPS) and SCALANCE XCM-/XRM-/XCH-/XRH-300 family (SINEC OS): If you have migrated your device(s) from SINEC OS to MSPS firmware or vice versa, please consider the respective measures in the MSPS or SINEC OS specific product families.

Description of the Vulnerability

The vulnerability could allow on-path attackers, located between a Network Access Server (the RADIUS client, e.g., SCALANCE or RUGGEDCOM devices) and a RADIUS server (e.g., SINEC INS), to forge Access-Request packets in a way that enables them to modify the corresponding server response packet at will, e.g., turning an “Access-Reject” message into an “Access-Accept”. This would cause the Network Access Server to grant the attackers access to the network with the attackers desired authorization (and without the need of knowing or guessing legitimate access credentials).

Successful attacks are demonstrated against RADIUS/UDP (IETF RFC 2865), similar attacks are considered possible against RADIUS/TCP (IETF RFC 6613). RADIUS/TLS (IETF RFC 6614) and RADIUS/DTLS (IETF RFC 7360) are not vulnerable.

Impact to SCALANCE and RUGGEDCOM Products, Countermeasures

SCALANCE and RUGGEDCOM devices use RADIUS/UDP and are therefore considered vulnerable, except for the IEEE 802.1X port security feature.

To fix the issue, specific countermeasures are required on both RADIUS client and RADIUS server side. In typical deployments, SCALANCE and RUGGEDCOM devices as well as RUGGEDCOM CROSSBOW are configured as RADIUS clients. SINEC INS as well as other 3rd party products are RADIUS servers.

RADIUS clients need to:

- C1. Ensure that all Access-Request packets they send to the server contain a Message-Authenticator attribute.
- C2. Implement a per-server configuration flag which requires that all Access-accept, Access-Reject, and Access-Challenge packets coming from a server must contain a Message-Authenticator attribute.

RADIUS servers need to:

- S1. Ensure that all replies to Access-Request packets contain a Message-Authenticator attribute as the first attribute in the packet.
- S2. Implement a per-client configuration flag which requires that all Access-Request packets coming from a client must contain a Message-Authenticator attribute.

- S3. If the server is also configured as a proxy (i.e., forwards certain client Access-Requests to another RADIUS server): Ensure that all proxied Access-Request packets contain a Message-Authenticator attribute.

The issue is fully mitigated only, if all recommendations are enforced in all RADIUS clients and servers. However, every individual recommendation decreases the likelihood of a successful attack.

Status

- **RUGGEDCOM CROSSBOW:** C1 is implemented in all versions; C2 is implemented in V5.6 or later.
- **RUGGEDCOM ROS V4.X family:** C1 and C2 are not implemented before V4.3.11; both are implemented in V4.3.11 or later. C2 can be configured from CLI / webUI at: `Administration -> Configure Security Server -> Configure RADIUS Server -> Select Server (primary and/or backup)-> Force Msg-Auth attr = (YES, NO)`. The default value of Force `Msg-Auth attr = NO`. If your RADIUS server supports the message authenticator attribute, it is recommended to set it to `YES`.
- **RUGGEDCOM ROS V5.X family:** C1 and C2 are not implemented before V5.10.0; both are implemented in V5.10.0 or later. C2 can be configured as described for the RUGGEDCOM ROS V4.X family.
- **RUGGEDCOM RST2428P:** C1 is implemented in all versions; C2 is implemented in V3.2 or later.
- **RUGGEDCOM devices, except the ones already listed above:** C1 and C2 are not implemented in current versions; both are planned to be implemented in a future version.
- **SCALANCE M-800 family (incl. S615, MUM-800 and RM1224):** C1 is implemented in all versions; C2 is implemented in V8.2 or later.
- **SCALANCE W-700 IEEE 802.11ax family:** C1 is implemented in all versions; C2 is implemented in V3.0.0 or later.
- **SCALANCE X-300 family (incl. X408 and SIPLUS NET variants):** C1 is implemented in V4.1.8 or later; C2 is implemented in V4.1.9 or later.
- **SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG family:** C1 is implemented in all versions; C2 is implemented in V4.6 or later.
- **SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 family:** C1 is implemented in all MSPS versions; C2 is implemented in MSPS V1.3 or later.
- **SCALANCE XCM-/XRM-/XCH-/XRH-300 family:** C1 is implemented in all SINEC OS versions; C2 is implemented in SINEC OS V3.2 or later.
- **SCALANCE devices, except the ones already listed above:** C1 is implemented in all versions; C2 is planned to be implemented in a future version.
- **SINEC INS, when RADIUS Server feature is enabled:** S1 is implemented in all versions for all clients that support C1; S2 is implemented in all versions.
- **SINEC INS, when the Relay feature is configured:** S3 is not implemented before V1.0 SP2 Update 4; S3 is implemented in V1.0 SP2 Update 4 or later.

Specific Countermeasures

- **RUGGEDCOM CROSSBOW:** Ensure that the RADIUS server(s) in your deployment implement S1-S3; ensure that S2 is enabled for RUGGEDCOM CROSSBOW; Update RUGGEDCOM CROSSBOW to V5.6 or later version to support C2. Alternatively, consider to use a different supported method for authentication: AD, RSA or a combination of both.
- **RUGGEDCOM ROS V4.X family:** Update to V4.3.11 or later version and consider the information in the Status section above.
- **RUGGEDCOM ROS V5.X family:** Update to V5.10.0 or later version and consider the information in the Status section above.
- **RUGGEDCOM RST2428P:** Update to V3.2 or later version and enforce by configuration that all packets coming from the RADIUS server contain a Message-Authenticator attribute (if the RADIUS server supports it).
- **RUGGEDCOM devices, except the ones already listed above:** Ensure that the RADIUS server(s) in your deployment implement S1-S3, but keep S2 disabled for RUGGEDCOM devices; as soon as a new firmware version is available that supports C1 and C2: update all devices and enable S2 on the server.

- **SCALANCE M-800 family (incl. S615, MUM-800 and RM1224):** Update to V8.2 or later version and enforce by configuration that all packets coming from the RADIUS server contain a Message-Authenticator attribute (if the RADIUS server supports it).
- **SCALANCE W-700 IEEE 802.11ax family:** Update to V3.0.0 or later version and enforce by configuration that all packets coming from the RADIUS server contain a Message-Authenticator attribute (if the RADIUS server supports it).
- **SCALANCE X-300 family (incl. X408 and SIPLUS NET variants):** Update to 4.1.9 or later version and enforce by configuration that all packets coming from the RADIUS server contain a Message-Authenticator attribute (if the RADIUS server supports it).
- **SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG family:** Update to 4.6 or later version and enforce by configuration that all packets coming from the RADIUS server contain a Message-Authenticator attribute (if the RADIUS server supports it).
- **SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 family:** Update to MSPS V1.3 or later version and enforce by configuration that all packets coming from the RADIUS server contain a Message-Authenticator attribute (if the RADIUS server supports it).
- **SCALANCE XCM-/XRM-/XCH-/XRH-300 family:** Update to SINEC OS V3.2 or later version and enforce by configuration that all packets coming from the RADIUS server contain a Message-Authenticator attribute (if the RADIUS server supports it).
- **SCALANCE devices, except the ones already listed above:** Update all devices to the latest available firmware version; ensure that the RADIUS server(s) in your deployment implement S1-S3; ensure that S2 is enabled for all SCALANCE devices; as soon as a new firmware version is available that supports C2: update all devices.
- **SINEC INS, when RADIUS Server feature is enabled:** Configure S2 for all clients that support C1.
- **SINEC INS, when the Relay feature is configured:** Update SINEC INS to V1.0 SP2 Update 4 or later version.

More Information

- CERT Coordination Center - “RADIUS protocol susceptible to forgery attacks": https://kb.cert.org/vuls/id/456537
- Research paper and related information - “RADIUS/UDP Considered Harmful": https://www.blastradius.fail/
- IETF Internet-Draft - “Deprecating Insecure Practices in RADIUS": https://datatracker.ietf.org/doc/draft-ietf-radext-deprecating-radius/

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 (2024-07-09):	Publication Date
V1.1 (2024-07-22):	Clarified that the fix for SCALANCE X-300 family (incl. X408 and SIPLUS NET variants) in V4.1.8 only covers RADIUS client mitigation C1, but not C2
V1.2 (2024-11-12):	Added fix for RUGGEDCOM CROSSBOW
V1.3 (2024-12-10):	Added fix (and related important recommendations in chapter Additional Information) for RUGGEDCOM ROS V4.x devices; Added additional SINEC OS-based devices as affected products: RUGGEDCOM RST2428P and SCALANCE XC-300, XR-300, XC-400 families, and additional devices in the SCALANCE XR-500 family
V1.4 (2025-01-14):	Added fix for SCALANCE W-700 IEEE 802.11ax family and for SCALANCE M-800 family (incl. S615, MUM-800 and RM1224)
V1.5 (2025-03-11):	Added fix for SCALANCE X-300 family (incl. X408 and SIPLUS NET variants)
V1.6 (2025-06-10):	Clarified that SINEC INS is only affected when the Relay feature is used; added fix for the RUGGEDCOM RST2428P, SCALANCE XC-300, SCALANCE XC-400 and SCALANCE XR-300 (6GK5334-xTSxx) families and for some of the devices in the SCALANCE XM-400/XR-500 and SCALANCE XCM-/XRM-/XCH-/XRH-300 families

V1.7 (2025-07-08): Added fix for SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG family, for SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 family (MSPS V1.3), for RUGGEDCOM ROS V5.X family and for SINEC INS (relay feature); Clarified the applicability of the MSPS V1.3 and the SINEC OS V3.2 fix releases for product families that support both

TERMS OF USE

The use of Siemens Security Advisories is subject to the terms and conditions listed on: https://www.siemens.com/productcert/terms-of-use.