# 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: 2024-07-09
Current Version: V1.0
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, the impact to SCALANCE, RUGGEDCOM and related products, specific countermeasures and external references can be found in the chapter “Additional Information”.

Siemens has released a new version for several products and recommends to update to the latest version. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| RUGGEDCOM CROSSBOW:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM ROS V4.X family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM i800:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM ROS V4.X NC products: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM i800NC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| RUGGEDCOM i801NC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM i802NC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM i803NC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM M2100NC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM M2200NC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM M969NC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RMC30NC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RMC8388NC V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RP110NC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS1600FNC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS1600NC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS1600TNC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| RUGGEDCOM RS400NC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS401NC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS416NC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS416NCv2 V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS416PNC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS416PNCv2 V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS8000ANC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS8000HNC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS8000NC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS8000TNC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900GNC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900GNC(32M) V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| RUGGEDCOM RS900GPNC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900MNC-GETS-C01:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900MNC-GETS-XX:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900MNC-STND-XX:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900MNC-STND-XX-C01:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900NC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900NC(32M) V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS910NC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS940GNC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2100NC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2100NC(32M) V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2100PNC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| RUGGEDCOM RSG2200NC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2288NC V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2300NC V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2300PNC V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2488NC V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG920PNC V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM i801:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM i802:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM i803:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM M2100:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM M2200:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM M969:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| RUGGEDCOM RMC30:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RMC8388 V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RP110:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS1600:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS1600F:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS1600T:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS400:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS401:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS416:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS416P:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS416Pv2 V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS416v2 V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| RUGGEDCOM RS8000:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS8000A:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS8000H:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS8000T:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900 (32M) V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900G:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900G (32M) V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900GP:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900M-GETS-C01:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900M-GETS-XX:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900M-STND-C01:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| RUGGEDCOM RS900M-STND-XX:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900W:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS910:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS910W:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS940G:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2100:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2100 (32M) V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2100P:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2200:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2288 V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2300 V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2300P V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| RUGGEDCOM RSG2488 V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG920P V4.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM ROS V5.X family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RMC8388 V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM ROS V5.X NC products: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RMC8388NC V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS416NCv2 V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS416PNCv2 V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900GNC(32M) V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900NC(32M) V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2100NC(32M) V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2288NC V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| RUGGEDCOM RSG2300NC V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2300PNC V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2488NC V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG920PNC V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSL910NC:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS416Pv2 V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS416v2 V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900 (32M) V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RS900G (32M) V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2100 (32M) V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2288 V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2300 V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| RUGGEDCOM RSG2300P V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG2488 V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG907R:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG908C:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG909R:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG910C:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSG920P V5.X:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RSL910:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RST2228:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RST2228P:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RST916C:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RST916P:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| RUGGEDCOM ROX II family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM ROX MX5000:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM ROX MX5000RE:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM ROX RX1400:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM ROX RX1500:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM ROX RX1501:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM ROX RX1510:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM ROX RX1511:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM ROX RX1512:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM ROX RX1524:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM ROX RX1536:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM ROX RX5000:<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE M-800 family (incl. S615, MUM-800 and RM1224): | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RM1224 family (6GK6108-4AM00): | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2):<br>All versions affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2):<br>All versions affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE M-800 family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE M804PB (6GK5804-0AP00-2AA2):<br>All versions affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE M812-1 ADSL-Router family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2):<br>All versions affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2):<br>All versions affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE M816-1 ADSL-Router family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2):<br>All versions affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2):<br>All versions affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE M874-2 (6GK5874-2AA00-2AA2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE M874-3 (6GK5874-3AA00-2AA2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE M876-3 (6GK5876-3AA02-2BA2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE M876-4 (6GK5876-4AA10-2BA2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE MUM-800 family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE S615 family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE SC-600 family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE SC622-2C (6GK5622-2GS00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE SC626-2C (6GK5626-2GS00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE SC632-2C (6GK5632-2GS00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE SC636-2C (6GK5636-2GS00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE SC642-2C (6GK5642-2GS00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE SC646-2C (6GK5646-2GS00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W-700 IEEE 802.11ax family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE WAM763-1 (6GK5763-1AL00-7DA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE WAM763-1 (ME) (6GK5763-1AL00-7DC0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE WAM763-1 (US) (6GK5763-1AL00-7DB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE WAM766-1 (EU) (6GK5766-1GE00-7DA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE WAM766-1 (ME) (6GK5766-1GE00-7DC0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE WAM766-1 (US) (6GK5766-1GE00-7DB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE WAM766-1 EEC (EU) (6GK5766-1GE00-7TA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE WAM766-1 EEC (ME) (6GK5766-1GE00-7TC0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE WAM766-1 EEC (US) (6GK5766-1GE00-7TB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE WUM763-1 (6GK5763-1AL00-3DA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE WUM763-1 (6GK5763-1AL00-3AA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE WUM763-1 (US) (6GK5763-1AL00-3AB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE WUM763-1 (US) (6GK5763-1AL00-3DB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE WUM766-1 (EU) (6GK5766-1GE00-3DA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE WUM766-1 (ME) (6GK5766-1GE00-3DC0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE WUM766-1 (US) (6GK5766-1GE00-3DB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W-700 IEEE 802.11n family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AC0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA6):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W734-1 RJ45 (USA) (6GK5734-1FX00-0AB6):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W738-1 M12 (6GK5738-1GY00-0AA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W738-1 M12 (6GK5738-1GY00-0AB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W748-1 M12 (6GK5748-1GD00-0AA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W748-1 M12 (6GK5748-1GD00-0AB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AC0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA6):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W774-1 RJ45 (USA) (6GK5774-1FX00-0AB6):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W778-1 M12 (6GK5778-1GY00-0AA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W778-1 M12 (6GK5778-1GY00-0AB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE W778-1 M12 EEC (6GK5778-1GY00-0TA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W778-1 M12 EEC (USA) (6GK5778-1GY00-0TB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AC0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W786-2 SFP (6GK5786-2FE00-0AA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W786-2 SFP (6GK5786-2FE00-0AB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AB0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W788-1 M12 (6GK5788-1GD00-0AA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

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

| | |
|---|---|
| SCALANCE W1748-1 M12 (6GK5748-1GY01-0TA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W1748-1 M12 (6GK5748-1GY01-0AA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W1788-1 M12 (6GK5788-1GY01-0AA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W1788-2 EEC M12 (6GK5788-2GY01-0TA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W1788-2 M12 (6GK5788-2GY01-0AA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE W1788-2IA M12 (6GK5788-2HY01-0AA0):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE X-300 family (incl. X408 and SIPLUS NET variants): | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X-300 EEC family: | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X302-7 EEC (230V, coated) (6GK5302-7GD00-3GA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X302-7 EEC (230V) (6GK5302-7GD00-3EA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE X302-7 EEC (24V, coated) (6GK5302-7GD00-1GA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X302-7 EEC (24V) (6GK5302-7GD00-1EA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X302-7 EEC (2x 230V, coated) (6GK5302-7GD00-4GA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X302-7 EEC (2x 230V) (6GK5302-7GD00-4EA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X302-7 EEC (2x 24V, coated) (6GK5302-7GD00-2GA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X302-7 EEC (2x 24V) (6GK5302-7GD00-2EA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-2 EEC (230V, coated) (6GK5307-2FD00-3GA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-2 EEC (230V) (6GK5307-2FD00-3EA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE X307-2 EEC (24V, coated) (6GK5307-2FD00-1GA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-2 EEC (24V) (6GK5307-2FD00-1EA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-2 EEC (2x 230V, coated) (6GK5307-2FD00-4GA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-2 EEC (2x 230V) (6GK5307-2FD00-4EA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-2 EEC (2x 24V, coated) (6GK5307-2FD00-2GA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-2 EEC (2x 24V) (6GK5307-2FD00-2EA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X-300 family: | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X304-2FE (6GK5304-2BD00-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE X306-1LD FE (6GK5306-1BF00-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X320-1 FE (6GK5320-1BD00-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X320-1-2LD FE (6GK5320-3BF00-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X300 family: | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-3 (6GK5307-3BL00-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-3LD (6GK5307-3BM00-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2 (6GK5308-2FL00-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2LD (6GK5308-2FM00-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE X308-2LH (6GK5308-2FN00-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2LH+ (6GK5308-2FP00-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X310 (6GK5310-0FA00-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X310FE (6GK5310-0BA00-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X-300 RD family: | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-3 (6GK5307-3BL10-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-3LD (6GK5307-3BM10-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2 RD (inkl. SIPLUS variants): | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE X308-2 (6GK5308-2FL10-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS NET SCALANCE X308-2 (6AG1308-2FL10-4AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2LD (6GK5308-2FM10-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2LH (6GK5308-2FN10-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2LH+ (6GK5308-2FP10-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X310 (6GK5310-0FA10-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X310FE (6GK5310-0BA10-2AA3):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2M family: | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE X308-2M (6GK5308-2GG00-2AA2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2M PoE (6GK5308-2QG00-2AA2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2M TS (6GK5308-2GG00-2CA2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2M RD family: | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2M (6GK5308-2GG10-2AA2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2M PoE (6GK5308-2QG10-2AA2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2M TS (6GK5308-2GG10-2CA2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X408 family: | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE X408-2 (6GK5408-2FD00-2AA2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR-300 family: | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-12M (230V, ports on front) (6GK5324-0GG00-3AR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-12M (230V, ports on rear) (6GK5324-0GG00-3HR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-12M (24V, ports on front) (6GK5324-0GG00-1AR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-12M (24V, ports on rear) (6GK5324-0GG00-1HR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-12M TS (24V) (6GK5324-0GG00-1CR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR-300 RD family: | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XR324-12M (230V, ports on front) (6GK5324-0GG10-3AR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-12M (230V, ports on rear) (6GK5324-0GG10-3HR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-12M (24V, ports on front) (6GK5324-0GG10-1AR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-12M (24V, ports on rear) (6GK5324-0GG10-1HR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-12M TS (24V) (6GK5324-0GG10-1CR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR-300 EEC family: | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front) (6GK5324-4GG00-3ER2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG00-3JR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XR324-4M EEC (24V, ports on front) (6GK5324-4GG00-1ER2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (24V, ports on rear) (6GK5324-4GG00-1JR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front) (6GK5324-4GG00-4ER2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG00-4JR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (2x 24V, ports on front) (6GK5324-4GG00-2ER2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (2x 24V, ports on rear) (6GK5324-4GG00-2JR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR-300 EEC RD family: | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front) (6GK5324-4GG10-3ER2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG10-3JR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (24V, ports on front) (6GK5324-4GG10-1ER2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (24V, ports on rear) (6GK5324-4GG10-1JR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front) (6GK5324-4GG10-4ER2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG10-4JR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (2x 24V, ports on front) (6GK5324-4GG10-2ER2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (2x 24V, ports on rear) (6GK5324-4GG10-2JR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR-300 POE family: | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XR324-4M PoE (230V, ports on front) (6GK5324-4QG00-3AR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M PoE (230V, ports on rear) (6GK5324-4QG00-3HR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M PoE (24V, ports on front) (6GK5324-4QG00-1AR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M PoE (24V, ports on rear) (6GK5324-4QG00-1HR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M PoE TS (24V, ports on front) (6GK5324-4QG00-1CR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR-300 POE RD family: | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M PoE (230V, ports on front) (6GK5324-4QG10-3AR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M PoE (230V, ports on rear) (6GK5324-4QG10-3HR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XR324-4M PoE (24V, ports on front) (6GK5324-4QG10-1AR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M PoE (24V, ports on rear) (6GK5324-4QG10-1HR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M PoE TS (24V, ports on front) (6GK5324-4QG10-1CR2):<br>All versions < V4.1.8<br>affected by CVE-2024-3596 | Update to V4.1.8 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109972408/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XB-200 family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XB205-3 (SC, PN) (6GK5205-3BB00-2AB2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XB205-3 (ST, E/IP) (6GK5205-3BD00-2TB2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XB205-3 (ST, E/IP) (6GK5205-3BB00-2TB2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XB205-3 (ST, PN) (6GK5205-3BD00-2AB2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XB205-3LD (SC, E/IP) (6GK5205-3BF00-2TB2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XB205-3LD (SC, PN) (6GK5205-3BF00-2AB2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XB208 (E/IP) (6GK5208-0BA00-2TB2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XB208 (PN) (6GK5208-0BA00-2AB2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XB213-3 (SC, E/IP) (6GK5213-3BD00-2TB2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XB213-3 (SC, PN) (6GK5213-3BD00-2AB2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XB213-3 (ST, E/IP) (6GK5213-3BB00-2TB2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XB213-3 (ST, PN) (6GK5213-3BB00-2AB2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XB213-3LD (SC, E/IP) (6GK5213-3BF00-2TB2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XB213-3LD (SC, PN) (6GK5213-3BF00-2AB2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XB216 (E/IP) (6GK5216-0BA00-2TB2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XB216 (PN) (6GK5216-0BA00-2AB2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC-200 family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC206-2 (SC) (6GK5206-2BD00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XC206-2 (ST/BFOC) (6GK5206-2BB00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC206-2G PoE (6GK5206-2RS00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC206-2G PoE (54 V DC) (6GK5206-2RS00-5AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC206-2G PoE EEC (54 V DC) (6GK5206-2RS00-5FC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC206-2SFP (6GK5206-2BS00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC206-2SFP EEC (6GK5206-2BS00-2FC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC206-2SFP G (6GK5206-2GS00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC206-2SFP G (EIP DEF.) (6GK5206-2GS00-2TC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC206-2SFP G EEC (6GK5206-2GS00-2FC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC208 (6GK5208-0BA00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC208EEC (6GK5208-0BA00-2FC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC208G (6GK5208-0GA00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XC208G (EIP def.) (6GK5208-0GA00-2TC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC208G EEC (6GK5208-0GA00-2FC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC208G PoE (6GK5208-0RA00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC208G PoE (54 V DC) (6GK5208-0RA00-5AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC216 (6GK5216-0BA00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC216-3G PoE (6GK5216-3RS00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC216-3G PoE (54 V DC) (6GK5216-3RS00-5AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC216-4C (6GK5216-4BS00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC216-4C G (6GK5216-4GS00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC216-4C G (EIP Def.) (6GK5216-4GS00-2TC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC216-4C G EEC (6GK5216-4GS00-2FC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC216EEC (6GK5216-0BA00-2FC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XC224 (6GK5224-0BA00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC224-4C G (6GK5224-4GS00-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC224-4C G (EIP Def.) (6GK5224-4GS00-2TC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XC224-4C G EEC (6GK5224-4GS00-2FC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS NET SCALANCE XC206-2 (6AG1206-2BB00-7AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS NET SCALANCE XC206-2SFP (6AG1206-2BS00-7AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS NET SCALANCE XC208 (6AG1208-0BA00-7AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS NET SCALANCE XC216-4C (6AG1216-4BS00-7AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XF-200BA family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XF204 (6GK5204-0BA00-2GF2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XF204 DNA (6GK5204-0BA00-2YF2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XF204-2BA (6GK5204-2AA00-2GF2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XF204-2BA DNA (6GK5204-2AA00-2YF2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XP-200 family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XP208 (6GK5208-0HA00-2AS6):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XP208 (Ethernet/IP) (6GK5208-0HA00-2TS6):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XP208EEC (6GK5208-0HA00-2ES6):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XP208PoE EEC (6GK5208-0UA00-5ES6):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XP216 (6GK5216-0HA00-2AS6):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XP216 (Ethernet/IP) (6GK5216-0HA00-2TS6):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XP216EEC (6GK5216-0HA00-2ES6):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XP216POE EEC (6GK5216-0UA00-5ES6):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR-300WG family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR324WG (24 x FE, AC 230V) (6GK5324-0BA00-3AR3):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XR324WG (24 X FE, DC 24V) (6GK5324-0BA00-2AR3):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR326-2C PoE WG (6GK5326-2QS00-3AR3):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR326-2C PoE WG (without UL) (6GK5326-2QS00-3RR3):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR328-4C WG (24XFE, 4XGE, 24V) (6GK5328-4FS00-2AR3):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR328-4C WG (24xFE, 4xGE,DC24V) (6GK5328-4FS00-2RR3):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR328-4C WG (24xFE,4xGE,AC230V) (6GK5328-4FS00-3AR3):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR328-4C WG (24xFE,4xGE,AC230V) (6GK5328-4FS00-3RR3):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR328-4C WG (28xGE, AC 230V) (6GK5328-4SS00-3AR3):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR328-4C WG (28xGE, DC 24V) (6GK5328-4SS00-2AR3):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XCM-/XRM-/XCH-/XRH-300 family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XCH328 (6GK5328-4TS01-2EC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XCM324 (6GK5324-8TS01-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XCM328 (6GK5328-4TS01-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XCM332 (6GK5332-0GA01-2AC2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XRH334 (24 V DC, 8xFO, CC) (6GK5334-2TS01-2ER3):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XRM334 (230 V AC, 12xFO) (6GK5334-3TS01-3AR3):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XRM334 (230 V AC, 8xFO) (6GK5334-2TS01-3AR3):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XRM334 (24 V DC, 12xFO) (6GK5334-3TS01-2AR3):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XRM334 (24 V DC, 8xFO) (6GK5334-2TS01-2AR3):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XRM334 (2x230 V AC, 12xFO) (6GK5334-3TS01-4AR3):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XRM334 (2x230 V AC, 8xFO) (6GK5334-2TS01-4AR3):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XM-400/XR-500 family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XM-400 family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XM408-4C (6GK5408-4GP00-2AM2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XM408-4C (L3 int.) (6GK5408-4GQ00-2AM2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XM408-8C (6GK5408-8GS00-2AM2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XM408-8C (L3 int.) (6GK5408-8GR00-2AM2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XM416-4C (6GK5416-4GS00-2AM2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XM416-4C (L3 int.) (6GK5416-4GR00-2AM2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR-500 family: | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR524-8C, 1x230V (6GK5524-8GS00-3AR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR524-8C, 1x230V (L3 int.) (6GK5524-8GR00-3AR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR524-8C, 24V (6GK5524-8GS00-2AR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR524-8C, 24V (L3 int.) (6GK5524-8GR00-2AR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR524-8C, 2x230V (6GK5524-8GS00-4AR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR524-8C, 2x230V (L3 int.) (6GK5524-8GR00-4AR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XR526-8C, 1x230V (6GK5526-8GS00-3AR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR526-8C, 1x230V (L3 int.) (6GK5526-8GR00-3AR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR526-8C, 24V (6GK5526-8GS00-2AR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR526-8C, 24V (L3 int.) (6GK5526-8GR00-2AR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR526-8C, 2x230V (6GK5526-8GS00-4AR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR526-8C, 2x230V (L3 int.) (6GK5526-8GR00-4AR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR528-6M (6GK5528-0AA00-2AR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR528-6M (2HR2, L3 int.) (6GK5528-0AR00-2HR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR528-6M (2HR2) (6GK5528-0AA00-2HR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR528-6M (L3 int.) (6GK5528-0AR00-2AR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR552-12M (6GK5552-0AA00-2AR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR552-12M (2HR2, L3 int.) (6GK5552-0AR00-2AR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XR552-12M (2HR2) (6GK5552-0AA00-2HR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE XR552-12M (2HR2) (6GK5552-0AR00-2HR2):<br>All versions<br>affected by CVE-2024-3596 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SINEC INS:<br>All versions when RADIUS Server feature is enabled<br>affected by CVE-2024-3596 | Currently no fix is planned<br>See 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:

- CVE-2024-3596:
  - 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
  - Restrict access to the networks where RADIUS messages are exchanged (e.g., send RADIUS traffic via management network or a dedicated VLAN)

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

## GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

## PRODUCT DESCRIPTION

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.

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

#### Description

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**

- **SCALANCE devices, except X-300 family (incl. X408 and SIPLUS NET variants)**: C1 is implemented in current firmware versions; C2 is planned to be implemented in a future version.
- **SCALANCE X-300 family (incl. X408 and SIPLUS NET variants)**: C1 and C2 are implemented in the latest firmware version (V4.1.8), but not supported in earlier versions.
- **RUGGEDCOM (ROX and ROS based) devices:** C1 and C2 are not supported in current firmware versions; both are planned to be implemented in a future version.
- **RUGGEDCOM CROSSBOW:** C1 is implemented in current firmware versions; C2 is planned to be implemented in a future version.
- **SINEC INS, when RADIUS Server feature is enabled:** S1 is implemented in current versions for all clients that support C1; S2 is implemented in current versions.
- **SINEC INS, when the Relay feature is configured:** S3 is not implemented, all packets are forwarded unchanged.

**Specific Countermeasures**

- **SCALANCE devices, except X-300 family (incl. X408 and SIPLUS NET variants):** 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.
- **SCALANCE X-300 family (incl. X408 and SIPLUS NET variants)**: Update all devices to V4.1.8 or later version; ensure that the RADIUS server(s) in your deployment implement S1-S3; ensure that S2 is enabled for all SCALANCE devices.
- **RUGGEDCOM (ROX and ROS based) devices:** 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 C2: update all devices and enable S2 on the server.
- **RUGGEDCOM CROSSBOW:** Update to the latest available version; ensure that the RADIUS server(s) in your deployment implement S1-S3; ensure that S2 is enabled for RUGGEDCOM CROSSBOW; as soon as a new version is available that supports C2: update RUGGEDCOM CROSSBOW. Alternatively, consider to use a different supported method for authentication: AD, RSA or a combination of both.
- **SINEC INS, when RADIUS Server feature is enabled:** Configure S2 for all clients that support C1
- **SINEC INS, when the Relay feature is configured:** Ensure that the connections between SINEC INS and the configured RADIUS server groups are secured and access-restricted (e.g. via IPSec or VPN)

**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

## TERMS OF USE