SSA-413565: Multiple Vulnerabilities in SCALANCE Products

Publication Date:	2022-12-13
Last Update:	2023-10-10
Current Version:	V1.3
CVSS v3.1 Base Score:	7.6

SUMMARY

Multiple SCALANCE devices are affected by several vulnerabilities that could allow an attacker to inject code, retrieve data as debug information as well as user CLI passwords or set the CLI to an irresponsive state.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE M804PB (6GK5804-0AP00-2AA2): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE M812-1 ADSL-Router (Annex A) (6GK5812-1AA00-2AA2): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE M812-1 ADSL-Router (Annex B) (6GK5812-1BA00-2AA2): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE M816-1 ADSL-Router (Annex A) (6GK5816-1AA00-2AA2): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE M816-1 ADSL-Router (Annex B) (6GK5816-1BA00-2AA2): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/

SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE M874-2 (6GK5874-2AA00-2AA2): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE M874-3 (6GK5874-3AA00-2AA2): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE M876-3 (EVDO) (6GK5876-3AA02-2BA2): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE M876-4 (6GK5876-4AA10-2BA2): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/

SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE S615 (6GK5615-0AA00-2AA2): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE S615 EEC (6GK5615-0AA01-2AA2): All versions < V7.2 affected by CVE-2022-34821, CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE SC622-2C (6GK5622-2GS00-2AC2): All versions < V2.3	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109805907/
SCALANCE SC622-2C (6GK5622-2GS00-2AC2): All versions >= V2.3 < V3.0 affected by CVE-2022-34821, CVE-2022-46142, CVE-2022-46143, CVE-2022-46144	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109814276/
SCALANCE SC626-2C (6GK5626-2GS00-2AC2): All versions < V2.3	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109805907/
SCALANCE SC626-2C (6GK5626-2GS00-2AC2): All versions >= V2.3 < V3.0 affected by CVE-2022-34821, CVE-2022-46142, CVE-2022-46143, CVE-2022-46144	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109814276/
SCALANCE SC632-2C (6GK5632-2GS00-2AC2): All versions < V2.3	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109805907/
SCALANCE SC632-2C (6GK5632-2GS00-2AC2): All versions >= V2.3 < V3.0 affected by CVE-2022-34821, CVE-2022-46142, CVE-2022-46143, CVE-2022-46144	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109814276/
SCALANCE SC636-2C (6GK5636-2GS00-2AC2): All versions < V2.3	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109805907/
SCALANCE SC636-2C (6GK5636-2GS00-2AC2): All versions >= V2.3 < V3.0 affected by CVE-2022-34821, CVE-2022-46142, CVE-2022-46143, CVE-2022-46144	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109814276/

SCALANCE SC642-2C (6GK5642-2GS00-2AC2): All versions < V2.3	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109805907/
SCALANCE SC642-2C (6GK5642-2GS00-2AC2): All versions >= V2.3 < V3.0 affected by CVE-2022-34821, CVE-2022-46142, CVE-2022-46143, CVE-2022-46144	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109814276/
SCALANCE SC646-2C (6GK5646-2GS00-2AC2): All versions < V2.3	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109805907/
SCALANCE SC646-2C (6GK5646-2GS00-2AC2): All versions >= V2.3 < V3.0 affected by CVE-2022-34821, CVE-2022-46142, CVE-2022-46143, CVE-2022-46144	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109814276/
SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AC0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned

SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA6): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W734-1 RJ45 (USA) (6GK5734-1FX00-0AB6): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W738-1 M12 (6GK5738-1GY00-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W738-1 M12 (6GK5738-1GY00-0AB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W748-1 M12 (6GK5748-1GD00-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W748-1 M12 (6GK5748-1GD00-0AB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned

SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA6): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AC0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W774-1 RJ45 (USA) (6GK5774-1FX00-0AB6): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W778-1 M12 (6GK5778-1GY00-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W778-1 M12 (6GK5778-1GY00-0AB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned

SCALANCE W778-1 M12 EEC (6GK5778-1GY00-0TA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W778-1 M12 EEC (USA) (6GK5778-1GY00-0TB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AC0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W786-2 SFP (6GK5786-2FE00-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W786-2 SFP (6GK5786-2FE00-0AB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned

SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W788-1 M12 (6GK5788-1GD00-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W788-1 M12 (6GK5788-1GD00-0AB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W788-2 M12 (6GK5788-2GD00-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W788-2 M12 (6GK5788-2GD00-0AB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TC0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned

SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AB0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AC0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W1748-1 M12 (6GK5748-1GY01-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W1748-1 M12 (6GK5748-1GY01-0TA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W1788-1 M12 (6GK5788-1GY01-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W1788-2 EEC M12 (6GK5788-2GY01-0TA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W1788-2 M12 (6GK5788-2GY01-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE W1788-2IA M12 (6GK5788-2HY01-0AA0): All versions affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Currently no fix is planned
SCALANCE WAM763-1 (6GK5763-1AL00-7DA0): All versions < V2.0 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109815650/

SCALANCE WAM763-1 (6GK5763-1AL00-7DA0): All versions affected by CVE-2022-34821	Currently no fix is planned
SCALANCE WAM766-1 (EU) (6GK5766-1GE00-7DA0): All versions < V2.0 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109815650/
SCALANCE WAM766-1 (EU) (6GK5766-1GE00-7DA0): All versions affected by CVE-2022-34821	Currently no fix is planned
SCALANCE WAM766-1 (US) (6GK5766-1GE00-7DB0): All versions < V2.0 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109815650/
SCALANCE WAM766-1 (US) (6GK5766-1GE00-7DB0): All versions affected by CVE-2022-34821	Currently no fix is planned
SCALANCE WAM766-1 EEC (EU) (6GK5766-1GE00-7TA0): All versions < V2.0 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109815650/
SCALANCE WAM766-1 EEC (EU) (6GK5766-1GE00-7TA0): All versions affected by CVE-2022-34821	Currently no fix is planned
SCALANCE WAM766-1 EEC (US) (6GK5766-1GE00-7TB0): All versions < V2.0 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109815650/
SCALANCE WAM766-1 EEC (US) (6GK5766-1GE00-7TB0): All versions affected by CVE-2022-34821	Currently no fix is planned
SCALANCE WUM763-1 (6GK5763-1AL00-3AA0): All versions < V2.0 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109815650/
SCALANCE WUM763-1 (6GK5763-1AL00-3AA0): All versions affected by CVE-2022-34821	Currently no fix is planned

SCALANCE WUM763-1 (6GK5763-1AL00-3DA0): All versions < V2.0 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109815650/
SCALANCE WUM763-1 (6GK5763-1AL00-3DA0): All versions affected by CVE-2022-34821	Currently no fix is planned
SCALANCE WUM766-1 (EU) (6GK5766-1GE00-3DA0): All versions < V2.0 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109815650/
SCALANCE WUM766-1 (EU) (6GK5766-1GE00-3DA0): All versions affected by CVE-2022-34821	Currently no fix is planned
SCALANCE WUM766-1 (US) (6GK5766-1GE00-3DB0): All versions < V2.0 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109815650/
SCALANCE WUM766-1 (US) (6GK5766-1GE00-3DB0): All versions affected by CVE-2022-34821	Currently no fix is planned
SCALANCE XB205-3 (SC, PN) (6GK5205-3BB00-2AB2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XB205-3 (ST, E/IP) (6GK5205-3BB00-2TB2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XB205-3 (ST, E/IP) (6GK5205-3BD00-2TB2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XB205-3 (ST, PN) (6GK5205-3BD00-2AB2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/

SCALANCE XB205-3LD (SC, E/IP) (6GK5205-3BF00-2TB2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XB205-3LD (SC, PN) (6GK5205-3BF00-2AB2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XB208 (E/IP) (6GK5208-0BA00-2TB2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XB208 (PN) (6GK5208-0BA00-2AB2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XB213-3 (SC, E/IP) (6GK5213-3BD00-2TB2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XB213-3 (SC, PN) (6GK5213-3BD00-2AB2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XB213-3 (ST, E/IP) (6GK5213-3BB00-2TB2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XB213-3 (ST, PN) (6GK5213-3BB00-2AB2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XB213-3LD (SC, E/IP) (6GK5213-3BF00-2TB2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XB213-3LD (SC, PN) (6GK5213-3BF00-2AB2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/

SCALANCE XB216 (E/IP) (6GK5216-0BA00-2TB2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XB216 (PN) (6GK5216-0BA00-2AB2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC206-2 (SC) (6GK5206-2BD00-2AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC206-2 (ST/BFOC) (6GK5206-2BB00-2AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC206-2G PoE (6GK5206-2RS00-2AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC206-2G PoE (54 V DC) (6GK5206-2RS00-5AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC206-2G PoE EEC (54 V DC) (6GK5206-2RS00-5FC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC206-2SFP (6GK5206-2BS00-2AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC206-2SFP EEC (6GK5206-2BS00-2FC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC206-2SFP G (6GK5206-2GS00-2AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/

SCALANCE XC206-2SFP G (EIP DEF.) (6GK5206-2GS00-2TC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC206-2SFP G EEC (6GK5206-2GS00-2FC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC208 (6GK5208-0BA00-2AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC208EEC (6GK5208-0BA00-2FC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC208G (6GK5208-0GA00-2AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC208G (EIP def.) (6GK5208-0GA00-2TC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC208G EEC (6GK5208-0GA00-2FC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC208G PoE (6GK5208-0RA00-2AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC208G PoE (54 V DC) (6GK5208-0RA00-5AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC216 (6GK5216-0BA00-2AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/

SCALANCE XC216-3G PoE (6GK5216-3RS00-2AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC216-3G PoE (54 V DC) (6GK5216-3RS00-5AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC216-4C (6GK5216-4BS00-2AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC216-4C G (6GK5216-4GS00-2AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC216-4C G (EIP Def.) (6GK5216-4GS00-2TC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC216-4C G EEC (6GK5216-4GS00-2FC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC216EEC (6GK5216-0BA00-2FC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC224 (6GK5224-0BA00-2AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC224-4C G (6GK5224-4GS00-2AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC224-4C G (EIP Def.) (6GK5224-4GS00-2TC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/

SCALANCE XC224-4C G EEC (6GK5224-4GS00-2FC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XF204 (6GK5204-0BA00-2GF2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XF204 DNA (6GK5204-0BA00-2YF2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XF204-2BA (6GK5204-2AA00-2GF2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XF204-2BA DNA (6GK5204-2AA00-2YF2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XM408-4C (6GK5408-4GP00-2AM2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XM408-4C (L3 int.) (6GK5408-4GQ00-2AM2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XM408-8C (6GK5408-8GS00-2AM2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XM408-8C (L3 int.) (6GK5408-8GR00-2AM2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XM416-4C (6GK5416-4GS00-2AM2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/

SCALANCE XM416-4C (L3 int.) (6GK5416-4GR00-2AM2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XP208 (6GK5208-0HA00-2AS6): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XP208 (Ethernet/IP) (6GK5208-0HA00-2TS6): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XP208EEC (6GK5208-0HA00-2ES6): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XP208PoE EEC (6GK5208-0UA00-5ES6): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XP216 (6GK5216-0HA00-2AS6): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XP216 (Ethernet/IP) (6GK5216-0HA00-2TS6): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XP216EEC (6GK5216-0HA00-2ES6): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XP216POE EEC (6GK5216-0UA00-5ES6): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XR324WG (24 x FE, AC 230V) (6GK5324-0BA00-3AR3): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/

SCALANCE XR324WG (24 X FE, DC 24V) (6GK5324-0BA00-2AR3): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XR326-2C PoE WG (6GK5326-2QS00-3AR3): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XR326-2C PoE WG (without UL) (6GK5326-2QS00-3RR3): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XR328-4C WG (24xFE,4xGE,AC230V) (6GK5328-4FS00-3AR3): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XR328-4C WG (24xFE,4xGE,AC230V) (6GK5328-4FS00-3RR3): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XR328-4C WG (24XFE, 4XGE, 24V) (6GK5328-4FS00-2AR3): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XR328-4C WG (24xFE, 4xGE,DC24V) (6GK5328-4FS00-2RR3): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XR328-4C WG (28xGE, AC 230V) (6GK5328-4SS00-3AR3): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XR328-4C WG (28xGE, DC 24V) (6GK5328-4SS00-2AR3): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/

SCALANCE XR524-8C, 1x230V (6GK5524-8GS00-3AR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XR524-8C, 1x230V (L3 int.) (6GK5524-8GR00-3AR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XR524-8C, 2x230V (6GK5524-8GS00-4AR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XR524-8C, 2x230V (L3 int.) (6GK5524-8GR00-4AR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XR524-8C, 24V (6GK5524-8GS00-2AR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XR524-8C, 24V (L3 int.) (6GK5524-8GR00-2AR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XR526-8C, 1x230V (6GK5526-8GS00-3AR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XR526-8C, 1x230V (L3 int.) (6GK5526-8GR00-3AR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XR526-8C, 2x230V (6GK5526-8GS00-4AR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XR526-8C, 2x230V (L3 int.) (6GK5526-8GR00-4AR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/

SCALANCE XR526-8C, 24V (6GK5526-8GS00-2AR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XR526-8C, 24V (L3 int.) (6GK5526-8GR00-2AR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XR528-6M (2HR2) (6GK5528-0AA00-2HR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XR528-6M (2HR2, L3 int.) (6GK5528-0AR00-2HR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XR528-6M (6GK5528-0AA00-2AR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XR528-6M (L3 int.) (6GK5528-0AR00-2AR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XR552-12M (2HR2) (6GK5552-0AA00-2HR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XR552-12M (2HR2) (6GK5552-0AR00-2HR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XR552-12M (2HR2, L3 int.) (6GK5552-0AR00-2AR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/
SCALANCE XR552-12M (6GK5552-0AA00-2AR2): All versions < V6.6 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109818003/

SIPLUS NET SCALANCE XC206-2 (6AG1206-2BB00-7AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SIPLUS NET SCALANCE XC206-2SFP (6AG1206-2BS00-7AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SIPLUS NET SCALANCE XC208 (6AG1208-0BA00-7AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SIPLUS NET SCALANCE XC216-4C (6AG1216-4BS00-7AC2): All versions < V4.4 affected by CVE-2022-46140, CVE-2022-46142, CVE-2022-46143	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/

WORKAROUNDS AND MITIGATIONS

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

GENERAL SECURITY RECOMMENDATIONS

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

PRODUCT DESCRIPTION

RUGGEDCOM RM1224 is a 4G ROUTER for wireless IP-communication from Ethernet based devices via LTE(4G)- mobile radio.

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).

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2022-34821

By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges.

CVSS v3.1 Base Score	7.6
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-94: Improper Control of Generation of Code ('Code Injection')

Vulnerability CVE-2022-46140

Affected devices use a weak encryption scheme to encrypt the debug zip file. This could allow an authenticated attacker to decrypt the contents of the file and retrieve debug information about the system.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-327: Use of a Broken or Risky Cryptographic Algorithm

Vulnerability CVE-2022-46142

Affected devices store the CLI user passwords encrypted in flash memory. Attackers with physical access to the device could retrieve the file and decrypt the CLI user passwords.

CVSS v3.1 Base Score	5.7
CVSS Vector	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-257: Storing Passwords in a Recoverable Format

Vulnerability CVE-2022-46143

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

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

Vulnerability CVE-2022-46144

Affected devices do not properly process CLI commands after a user forcefully quitted the SSH connection. This could allow an authenticated attacker to make the CLI via SSH or serial interface irresponsive.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-664: Improper Control of a Resource Through its Lifetime

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2022-12-13):	Publication Date
V1.1 (2023-03-14):	Added fix for SCALANCE WxM-700 family, RUGGEDCOM RM1224 family, SCALANCE M-800 family, SCALANCE MUM-800 family and SCALANCE S615 family
V1.2 (2023-04-11):	Added fix to SCALANCE XB-200, XC-200, XP-200, XF-200BA, XR-300WG and XR-500 families
V1.3 (2023-10-10):	Removed SCALANCE WAM766-1 6GHz devices with MLFBs 6GK5766-1JE00 as they are currently still unreleased, updated CVE-2022-34821 still unfixed and no fix planned for SCALANCE W-700 IEEE 802.11ax family

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.