SSA-244969: OpenSSL Vulnerability in Industrial Products

Publication Date:	2022-02-08
Last Update:	2022-02-08
Current Version:	V1.0
CVSS v3.1 Base Score:	7.4

SUMMARY

OpenSSL has published a security advisory [0] about a vulnerability in OpenSSL versions 1.1.1 < 1.1.1l and 1.0.2 < 1.0.2za that allows an attacker to cause a denial of service (DoS) or to disclose private memory content.

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

[0] https://www.openssl.org/news/secadv/20210824.txt

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX MX5000: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX MX5000RE: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1400: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1500: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1501: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1510: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1511: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations

RUGGEDCOM ROX RX1512: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1524: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1536: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX5000: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE M804PB (6GK5804-0AP00-2AA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE M812-1 ADSL-Router (Annex A) (6GK5812-1AA00-2AA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE M812-1 ADSL-Router (Annex B) (6GK5812-1BA00-2AA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE M816-1 ADSL-Router (Annex A) (6GK5816-1AA00-2AA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE M816-1 ADSL-Router (Annex B) (6GK5816-1BA00-2AA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE M874-2 (6GK5874-2AA00-2AA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE M874-3 (6GK5874-3AA00-2AA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE M876-3 (6GK5876-3AA02-2BA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations

SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE S615 (6GK5615-0AA00-2AA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
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 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 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 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 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 W721-1 RJ45 (6GK5721-1FC00-0AA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AC0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations

SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA6): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W734-1 RJ45 (USA) (6GK5734-1FX00-0AB6): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE W738-1 M12 (6GK5738-1GY00-0AA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W738-1 M12 (6GK5738-1GY00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W748-1 M12 (6GK5748-1GD00-0AA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W748-1 M12 (6GK5748-1GD00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations

SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA6): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AC0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (USA) (6GK5774-1FX00-0AB6): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE W778-1 M12 (6GK5778-1GY00-0AA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W778-1 M12 (6GK5778-1GY00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W778-1 M12 EEC (6GK5778-1GY00-0TA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W778-1 M12 EEC (USA) (6GK5778-1GY00-0TB0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations

SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AC0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 SFP (6GK5786-2FE00-0AA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 SFP (6GK5786-2FE00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-1 M12 (6GK5788-1GD00-0AA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-1 M12 (6GK5788-1GD00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 (6GK5788-2GD00-0AA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 (6GK5788-2GD00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations

SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TC0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AA0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AC0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SCALANCE W1748-1 M12 (6GK5748-1GY01-0AA0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE W1748-1 M12 (6GK5748-1GY01-0TA0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE W1788-1 M12 (6GK5788-1GY01-0AA0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE W1788-2 EEC M12 (6GK5788-2GY01-0TA0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE W1788-2 M12 (6GK5788-2GY01-0AA0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE W1788-2IA M12 (6GK5788-2HY01-0AA0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 (6GK5766-1GE00-7DA0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 (6GK5766-1GE00-7DB0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations

SCALANCE WAM766-1 6GHz (6GK5766-1JE00-7DA0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 EEC (6GK5766-1GE00-7TA0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 EEC (6GK5766-1GE00-7TB0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 EEC 6GHz (6GK5766-1JE00-7TA0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE WUM766-1 (6GK5766-1GE00-3DA0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE WUM766-1 (6GK5766-1GE00-3DB0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE WUM766-1 6GHz (6GK5766-1JE00-3DA0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X200-4 P IRT: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X201-3P IRT: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X201-3P IRT PRO: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X202-2 IRT: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X202-2P IRT (incl. SIPLUS NET variant): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X202-2P IRT PRO: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X204 IRT: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X204 IRT PRO: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations

SCALANCE X204-2 (6GK5204-2BB10-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X204-2FM (6GK5204-2BB11-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X204-2LD (6GK5204-2BC10-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X204-2LD TS (6GK5204-2BC10-2CA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X204-2TS (6GK5204-2BB10-2CA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X206-1 (6GK5206-1BB10-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X206-1LD (6GK5206-1BC10-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X208 (6GK5208-0BA10-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X208PRO (6GK5208-0HA10-2AA6): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X212-2 (6GK5212-2BB00-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X212-2LD (6GK5212-2BC00-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X216 (6GK5216-0BA00-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X224 (6GK5224-0BA00-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (2x 24V) (6GK5302-7GD00-2EA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations

SCALANCE X302-7 EEC (2x 24V, coated) (6GK5302-7GD00-2GA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (2x 230V) (6GK5302-7GD00-4EA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (2x 230V, coated) (6GK5302-7GD00-4GA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (24V) (6GK5302-7GD00-1EA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (24V, coated) (6GK5302-7GD00-1GA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (230V) (6GK5302-7GD00-3EA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (230V, coated) (6GK5302-7GD00-3GA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X304-2FE (6GK5304-2BD00-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X306-1LD FE (6GK5306-1BF00-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (2x 24V) (6GK5307-2FD00-2EA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (2x 24V, coated) (6GK5307-2FD00-2GA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (2x 230V) (6GK5307-2FD00-4EA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (2x 230V, coated) (6GK5307-2FD00-4GA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations

SCALANCE X307-2 EEC (24V) (6GK5307-2FD00-1EA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (24V, coated) (6GK5307-2FD00-1GA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (230V) (6GK5307-2FD00-3EA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (230V, coated) (6GK5307-2FD00-3GA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X307-3 (6GK5307-3BL00-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X307-3 (6GK5307-3BL10-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X307-3LD (6GK5307-3BM00-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X307-3LD (6GK5307-3BM10-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X308-2 (6GK5308-2FL00-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X308-2 (6GK5308-2FL10-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X308-2LD (6GK5308-2FM00-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X308-2LD (6GK5308-2FM10-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH (6GK5308-2FN00-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH (6GK5308-2FN10-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations

SCALANCE X308-2LH+ (6GK5308-2FP00-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH+ (6GK5308-2FP10-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X308-2M (6GK5308-2GG00-2AA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X308-2M (6GK5308-2GG10-2AA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X308-2M PoE (6GK5308-2QG00-2AA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X308-2M PoE (6GK5308-2QG10-2AA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X308-2M TS (6GK5308-2GG00-2CA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X308-2M TS (6GK5308-2GG10-2CA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X310 (6GK5310-0FA00-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X310 (6GK5310-0FA10-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X310FE (6GK5310-0BA10-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X320-1 FE (6GK5320-1BD00-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X320-1-2LD FE (6GK5320-3BF00-2AA3): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE X408-2 (6GK5408-2FD00-2AA2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations

SCALANCE X-300 switch family (incl. X408 and SIPLUS NET variants): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XF201-3P IRT: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XF202-2P IRT: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XF204 (6GK5204-0BA00-2AF2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XF204 IRT: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XF204-2 (6GK5204-2BC00-2AF2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XF204-2BA IRT: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XF206-1 (6GK5206-1BC00-2AF2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XF208 (6GK5208-0BA00-2AF2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front) (6GK5324-4GG00-4ER2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front) (6GK5324-4GG10-4ER2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG00-4JR2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (24V, ports on front) (6GK5324-4GG00-1ER2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (24V, ports on front) (6GK5324-4GG10-1ER2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations

SCALANCE XR324-4M EEC (24V, ports on rear) (6GK5324-4GG00-1JR2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (24V, ports on rear) (6GK5324-4GG10-1JR2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front) (6GK5324-4GG00-3ER2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front) (6GK5324-4GG10-3ER2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG00-3JR2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG10-3JR2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (24V, ports on front) (6GK5324-0GG00-1AR2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (24V, ports on front) (6GK5324-0GG10-1AR2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (24V, ports on rear) (6GK5324-0GG00-1HR2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (24V, ports on rear) (6GK5324-0GG10-1HR2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (230V, ports on front) (6GK5324-0GG00-3AR2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (230V, ports on front) (6GK5324-0GG10-3AR2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (230V, ports on rear) (6GK5324-0GG00-3HR2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations

SCALANCE XR324-12M (230V, ports on rear) (6GK5324-0GG10-3HR2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M TS (24V) (6GK5324-0GG00-1CR2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M TS (24V) (6GK5324-0GG10-1CR2): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1242-7 GPRS V2 (6GK7242-7KX31-0XE0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-1 (6GK7243-1BX30-0XE0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-7 LTE EU (6GK7243-7KX30-0XE0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-7 LTE US (6GK7243-7SX30-0XE0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1542SP-1 (6GK7542-6UX00-0XE0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 1543-1 (6GK7543-1AX00-0XE0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1545-1 (6GK7545-1GX00-0XE0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SIMATIC PCS neo: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SIMATIC Process Historian OPC UA Server: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations

SINEC NMS: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SINEMA Remote Connect Server: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SINEMA Server V14: All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SINUMERIK Operate: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SIPLUS NET CP 1543-1 (6AG1543-1AX00-2XE0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SIPLUS S7-1200 CP 1243-1 (6AG1243-1BX30-2AX0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SIPLUS S7-1200 CP 1243-1 RAIL (6AG2243-1BX30-1XE0): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
TIA Administrator: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific workarounds or mitigations. Please follow the General Security Recommendations.

Product specific mitigations can be found in the section Affected Products and Solution.

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

Products of the SIMATIC S7-1200 CPU family have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

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

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

SCALANCE W-700 products are wireless communication devices based on IEEE 802.11 standards. 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-1700 products are wireless communication devices based on IEEE 802.11 standards. 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).

SIMATIC PCS neo is a distributed control system (DCS).

SIMATIC Process Historian is the long term archive system for SIMATIC PCS 7, SIMATIC WinCC and SIMATIC PCS neo. It stores process values, alarms and batch data of production plants in its database and offers historical process data to reporting and visualization applications.

SINEC NMS is a new generation of the Network Management System (NMS) for the Digital Enterprise. This system can be used to centrally monitor, manage, and configure networks.

SINEMA Remote Connect is a management platform for remote networks that enables the simple management of tunnel connections (VPN) between headquarters, service technicians, and installed machines or plants. It provides both the Remote Connect Server, which is the server application, and the Remote Connect Client, which is an OpenVPN client for optimal connection to SINEMA Remote Connect Server.

SINEMA Server is a network monitoring and management software designed by Siemens for use in Industrial Ethernet networks.

SINUMERIK Operate is a standard Human-Machine-Interface system for SINUMERIK numerical controls.

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

The SCALANCE M-800, MUM-800 and S615 as well as the RUGGEDCOM RM1224 industrial routers are used for secure remote access to plants via mobile networks, e.g. GPRS or UMTS with the integrated security functions of a firewall for protection against unauthorized access and VPN to protect data transmission.

The SCALANCE SC-600 devices (SC622-2C, SC632-2C, SC636-2C, SC642-2C, SC646-2C) are used to protect trusted industrial networks from untrusted networks. They allow filtering incoming and outgoing network connections in different ways.

The SIMATIC CP 1242-7 and CP 1243-7 LTE communication processors connect the S7-1200 controller to Wide Area Networks (WAN). It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

The SIMATIC CP 1243-1 communication processor connects the S7-1200 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

The SIMATIC CP 1243-8 IRC communication processor connects S7-1200 controllers via the SINAUT ST7 telecontrol protocol to a control center or master ST7 stations.

The SIMATIC CP 1543-1, CP 1543SP-1, CP 1542SP-1 and CP 1542SP-1 IRC communication processors connects the S7-1500 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

The SIMATIC CP 1545-1 communication processor connects the S7-1500 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption. The communication processor protects S7-1500 stations against unauthorized access, as well as integrity and confidentiality of transmitted data.

TIA Administrator is a web-based framework that can incorporate different function modules for administrative tasks, as well as functions for managing SIMATIC software and licenses.

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-2021-3712

ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

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 (2022-02-08):	Publication Date

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.