SSA-712929: Denial of Service Vulnerability in OpenSSL (CVE-2022-0778) Affecting Industrial Products

Publication Date:	2022-06-14
Last Update:	2024-07-09
Current Version:	V2.8
CVSS v3.1 Base Score:	7.5
CVSS v4.0 Base Score:	8.7

SUMMARY

A vulnerability in the openSSL component (CVE-2022-0778, [0]) could allow an attacker to create a denial of service condition by providing specially crafted elliptic curve certificates to products that use a vulnerable version of openSSL.

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

[0] https://www.openssl.org/news/secadv/20220315.txt

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Industrial Edge - OPC UA Connector: All versions < V1.7 affected by CVE-2022-0778	Use the Edge Management System to update to V1.7 or later version https://www.siemens.com/industrial-edge-marketplace/
Industrial Edge - SIMATIC S7 Connector App: All versions < V1.7 affected by CVE-2022-0778	Use the Edge Management System to update to V1.7 or later version https://www.siemens.com/industrial-edge-marketplace/
OpenPCS 7 V8.2: All versions (OPC UA interface only) affected by CVE-2022-0778	Currently no fix is planned Restrict access to the OPC UA interface to trusted systems
OpenPCS 7 V9.0: All versions (OPC UA interface only) affected by CVE-2022-0778	Currently no fix is planned Restrict access to the OPC UA interface to trusted systems
OpenPCS 7 V9.1: All versions (OPC UA interface only) affected by CVE-2022-0778	Currently no fix is planned Restrict access to the OPC UA interface to trusted systems
RUGGEDCOM CROSSBOW Station Access Controller (SAC): All versions only when running on ROX II < V2.15.1 affected by CVE-2022-0778	Update ROX II to V2.15.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810800/

RUGGEDCOM ROX II family:	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810800/
RUGGEDCOM ROX MX5000: All versions < V2.15.1 affected by CVE-2022-0778	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810800/
RUGGEDCOM ROX MX5000RE: All versions < V2.15.1 affected by CVE-2022-0778	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810800/
RUGGEDCOM ROX RX1400: All versions < V2.15.1 affected by CVE-2022-0778	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810800/
RUGGEDCOM ROX RX1500: All versions < V2.15.1 affected by CVE-2022-0778	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810800/
RUGGEDCOM ROX RX1501: All versions < V2.15.1 affected by CVE-2022-0778	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810800/
RUGGEDCOM ROX RX1510: All versions < V2.15.1 affected by CVE-2022-0778	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810800/
RUGGEDCOM ROX RX1511: All versions < V2.15.1 affected by CVE-2022-0778	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810800/
RUGGEDCOM ROX RX1512: All versions < V2.15.1 affected by CVE-2022-0778	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810800/
RUGGEDCOM ROX RX1524: All versions < V2.15.1 affected by CVE-2022-0778	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810800/
RUGGEDCOM ROX RX1536: All versions < V2.15.1 affected by CVE-2022-0778	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810800/
RUGGEDCOM ROX RX5000: All versions < V2.15.1 affected by CVE-2022-0778	Update to V2.15.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810800/

SCALANCE LPE9403 (6GK5998-3GS00-2AC2): All versions < V2.0 affected by CVE-2022-0778	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109811123/
SCALANCE M-800 family (incl. S615, MUM-800 and RM1224):	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
RUGGEDCOM RM1224 family (6GK6108-4AM00):	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2): All versions < V7.2 affected by CVE-2022-0778	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-2022-0778	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE M-800 family:	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-2022-0778	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE M812-1 ADSL-Router family:	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2): All versions < V7.2 affected by CVE-2022-0778	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2): All versions < V7.2 affected by CVE-2022-0778	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE M816-1 ADSL-Router family:	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2): All versions < V7.2 affected by CVE-2022-0778	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/

SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2): All versions < V7.2 affected by CVE-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE M876-3 (6GK5876-3AA02-2BA2): All versions < V7.2 affected by CVE-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE MUM-800 family:	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-2022-0778	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-2022-0778	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-2022-0778	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE S615 family:	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2): All versions < V7.2 affected by CVE-2022-0778	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2): All versions < V7.2 affected by CVE-2022-0778	Update to V7.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817007/
SCALANCE SC-600 family:	Update to V2.3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810992/
SCALANCE SC622-2C (6GK5622-2GS00-2AC2): All versions < V2.3.1 affected by CVE-2022-0778	Update to V2.3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810992/
SCALANCE SC632-2C (6GK5632-2GS00-2AC2): All versions < V2.3.1 affected by CVE-2022-0778	Update to V2.3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810992/
SCALANCE SC636-2C (6GK5636-2GS00-2AC2): All versions < V2.3.1 affected by CVE-2022-0778	Update to V2.3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810992/
SCALANCE SC642-2C (6GK5642-2GS00-2AC2): All versions < V2.3.1 affected by CVE-2022-0778	Update to V2.3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810992/
SCALANCE SC646-2C (6GK5646-2GS00-2AC2): All versions < V2.3.1 affected by CVE-2022-0778	Update to V2.3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810992/
SCALANCE W1750D family:	Update to V8.7.1.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109816886/
SCALANCE W1750D (JP) (6GK5750-2HX01-1AD0): All versions < V8.7.1.11 affected by CVE-2022-0778	Update to V8.7.1.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109816886/

SCALANCE W1750D (ROW) (6GK5750-2HX01-1AA0): All versions < V8.7.1.11 affected by CVE-2022-0778	Update to V8.7.1.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109816886/
SCALANCE W1750D (USA) (6GK5750-2HX01-1AB0): All versions < V8.7.1.11 affected by CVE-2022-0778	Update to V8.7.1.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109816886/
SCALANCE W-700 IEEE 802.11ax family:	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 < V2.0 affected by CVE-2022-0778	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 < V2.0 affected by CVE-2022-0778	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 < V2.0 affected by CVE-2022-0778	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 < V2.0 affected by CVE-2022-0778	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 < V2.0 affected by CVE-2022-0778	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 < V2.0 affected by CVE-2022-0778	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 < V2.0 affected by CVE-2022-0778	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 < V2.0 affected by CVE-2022-0778	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 < V2.0 affected by CVE-2022-0778	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109815650/
SCALANCE W-700 IEEE 802.11n family:	Currently no fix is planned

SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AA0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AA0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AC0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA6): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W734-1 RJ45 (USA) (6GK5734-1FX00-0AB6): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W738-1 M12 (6GK5738-1GY00-0AA0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W738-1 M12 (6GK5738-1GY00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W748-1 M12 (6GK5748-1GD00-0AA0): All versions affected by CVE-2022-0778	Currently no fix is planned

SCALANCE W748-1 M12 (6GK5748-1GD00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AA0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AA0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TA0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA6): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AC0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W774-1 RJ45 (USA) (6GK5774-1FX00-0AB6): All versions affected by CVE-2022-0778	Currently no fix is planned

SCALANCE W778-1 M12 (6GK5778-1GY00-0AA0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W778-1 M12 (6GK5778-1GY00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W778-1 M12 EEC (6GK5778-1GY00-0TA0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W778-1 M12 EEC (USA) (6GK5778-1GY00-0TB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AA0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AA0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AC0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W786-2 SFP (6GK5786-2FE00-0AA0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W786-2 SFP (6GK5786-2FE00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AA0): All versions affected by CVE-2022-0778	Currently no fix is planned

SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W788-1 M12 (6GK5788-1GD00-0AA0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W788-1 M12 (6GK5788-1GD00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AA0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W788-2 M12 (6GK5788-2GD00-0AA0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W788-2 M12 (6GK5788-2GD00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TA0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TC0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AA0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned

SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AC0): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE W-1700 IEEE 802.11ac family:	Currently no fix is available
SCALANCE W1748-1 M12 (6GK5748-1GY01-0AA0): All versions affected by CVE-2022-0778	Currently no fix is available
SCALANCE W1748-1 M12 (6GK5748-1GY01-0TA0): All versions affected by CVE-2022-0778	Currently no fix is available
SCALANCE W1788-1 M12 (6GK5788-1GY01-0AA0): All versions affected by CVE-2022-0778	Currently no fix is available
SCALANCE W1788-2 EEC M12 (6GK5788-2GY01-0TA0): All versions affected by CVE-2022-0778	Currently no fix is available
SCALANCE W1788-2 M12 (6GK5788-2GY01-0AA0): All versions affected by CVE-2022-0778	Currently no fix is available
SCALANCE W1788-2IA M12 (6GK5788-2HY01-0AA0): All versions affected by CVE-2022-0778	Currently no fix is available
SCALANCE X200-4P IRT (6GK5200-4AH00-2BA3): All versions < V5.5.2 affected by CVE-2022-0778	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE X201-3P IRT (6GK5201-3BH00-2BA3): All versions < V5.5.2 affected by CVE-2022-0778	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE X201-3P IRT PRO (6GK5201-3JR00-2BA6): All versions < V5.5.2 affected by CVE-2022-0778	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE X202-2IRT (6GK5202-2BB00-2BA3): All versions < V5.5.2 affected by CVE-2022-0778	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/

SCALANCE X202-2IRT (6GK5202-2BB10-2BA3): All versions < V5.5.2 affected by CVE-2022-0778	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE X202-2P IRT (6GK5202-2BH00-2BA3): All versions < V5.5.2 affected by CVE-2022-0778	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE X202-2P IRT PRO (6GK5202-2JR00-2BA6): All versions < V5.5.2 affected by CVE-2022-0778	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE X204-2 (6GK5204-2BB10-2AA3): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE X204-2FM (6GK5204-2BB11-2AA3): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE X204-2LD (6GK5204-2BC10-2AA3): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE X204-2LD TS (6GK5204-2BC10-2CA2): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE X204-2TS (6GK5204-2BB10-2CA2): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE X204IRT (6GK5204-0BA00-2BA3): All versions < V5.5.2 affected by CVE-2022-0778	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE X204IRT (6GK5204-0BA10-2BA3): All versions < V5.5.2 affected by CVE-2022-0778	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE X204IRT PRO (6GK5204-0JA00-2BA6): All versions < V5.5.2 affected by CVE-2022-0778	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE X206-1 (6GK5206-1BB10-2AA3): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE X206-1LD (6GK5206-1BC10-2AA3): All versions affected by CVE-2022-0778	Currently no fix is planned

SCALANCE X208 (6GK5208-0BA10-2AA3): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE X208PRO (6GK5208-0HA10-2AA6): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE X212-2 (6GK5212-2BB00-2AA3): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE X212-2LD (6GK5212-2BC00-2AA3): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE X216 (6GK5216-0BA00-2AA3): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE X224 (6GK5224-0BA00-2AA3): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE X-300 family (incl. X408 and SIPLUS NET variants):	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X-300 EEC family:	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X302-7 EEC (230V, coated) (6GK5302-7GD00-3GA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X302-7 EEC (230V) (6GK5302-7GD00-3EA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X302-7 EEC (24V, coated) (6GK5302-7GD00-1GA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X302-7 EEC (24V) (6GK5302-7GD00-1EA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X302-7 EEC (2x 230V, coated) (6GK5302-7GD00-4GA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/

SCALANCE X302-7 EEC (2x 230V) (6GK5302-7GD00-4EA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X302-7 EEC (2x 24V, coated) (6GK5302-7GD00-2GA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X302-7 EEC (2x 24V) (6GK5302-7GD00-2EA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X307-2 EEC (230V, coated) (6GK5307-2FD00-3GA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X307-2 EEC (230V) (6GK5307-2FD00-3EA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X307-2 EEC (24V, coated) (6GK5307-2FD00-1GA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X307-2 EEC (24V) (6GK5307-2FD00-1EA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X307-2 EEC (2x 230V, coated) (6GK5307-2FD00-4GA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X307-2 EEC (2x 230V) (6GK5307-2FD00-4EA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X307-2 EEC (2x 24V, coated) (6GK5307-2FD00-2GA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X307-2 EEC (2x 24V) (6GK5307-2FD00-2EA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X-300 family:	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/

SCALANCE X304-2FE (6GK5304-2BD00-2AA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X306-1LD FE (6GK5306-1BF00-2AA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X320-1 FE (6GK5320-1BD00-2AA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X320-1-2LD FE (6GK5320-3BF00-2AA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X300 family:	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X307-3 (6GK5307-3BL00-2AA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X307-3LD (6GK5307-3BM00-2AA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X308-2 (6GK5308-2FL00-2AA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X308-2LD (6GK5308-2FM00-2AA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X308-2LH (6GK5308-2FN00-2AA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X308-2LH+ (6GK5308-2FP00-2AA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X310 (6GK5310-0FA00-2AA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/

SCALANCE X310FE (6GK5310-0BA00-2AA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X-300 RD family:	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X307-3 (6GK5307-3BL10-2AA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X307-3LD (6GK5307-3BM10-2AA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X308-2 RD (inkl. SIPLUS variants): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X308-2LD (6GK5308-2FM10-2AA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X308-2LH (6GK5308-2FN10-2AA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X308-2LH+ (6GK5308-2FP10-2AA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X310 (6GK5310-0FA10-2AA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X310FE (6GK5310-0BA10-2AA3): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X308-2M family:	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X308-2M (6GK5308-2GG00-2AA2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/

SCALANCE X308-2M PoE (6GK5308-2QG00-2AA2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X308-2M TS (6GK5308-2GG00-2CA2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X308-2M RD family:	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X308-2M (6GK5308-2GG10-2AA2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X308-2M PoE (6GK5308-2QG10-2AA2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X308-2M TS (6GK5308-2GG10-2CA2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X408 family:	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE X408-2 (6GK5408-2FD00-2AA2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR-300 family:	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-12M (230V, ports on front) (6GK5324-0GG00-3AR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-12M (230V, ports on rear) (6GK5324-0GG00-3HR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-12M (24V, ports on front) (6GK5324-0GG00-1AR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/

SCALANCE XR324-12M (24V, ports on rear) (6GK5324-0GG00-1HR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-12M TS (24V) (6GK5324-0GG00-1CR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR-300 RD family:	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-12M (230V, ports on front) (6GK5324-0GG10-3AR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-12M (230V, ports on rear) (6GK5324-0GG10-3HR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-12M (24V, ports on front) (6GK5324-0GG10-1AR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-12M (24V, ports on rear) (6GK5324-0GG10-1HR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-12M TS (24V) (6GK5324-0GG10-1CR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR-300 EEC family:	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front) (6GK5324-4GG00-3ER2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG00-3JR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M EEC (24V, ports on front) (6GK5324-4GG00-1ER2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/

SCALANCE XR324-4M EEC (24V, ports on rear) (6GK5324-4GG00-1JR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front) (6GK5324-4GG00-4ER2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG00-4JR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M EEC (2x 24V, ports on front) (6GK5324-4GG00-2ER2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M EEC (2x 24V, ports on rear) (6GK5324-4GG00-2JR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR-300 EEC RD family:	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front) (6GK5324-4GG10-3ER2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG10-3JR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M EEC (24V, ports on front) (6GK5324-4GG10-1ER2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M EEC (24V, ports on rear) (6GK5324-4GG10-1JR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front) (6GK5324-4GG10-4ER2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/

SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG10-4JR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M EEC (2x 24V, ports on front) (6GK5324-4GG10-2ER2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M EEC (2x 24V, ports on rear) (6GK5324-4GG10-2JR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR-300 POE family:	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M PoE (230V, ports on front) (6GK5324-4QG00-3AR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M PoE (230V, ports on rear) (6GK5324-4QG00-3HR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M PoE (24V, ports on front) (6GK5324-4QG00-1AR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M PoE (24V, ports on rear) (6GK5324-4QG00-1HR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M PoE TS (24V, ports on front) (6GK5324-4QG00-1CR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR-300 POE RD family:	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M PoE (230V, ports on front) (6GK5324-4QG10-3AR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M PoE (230V, ports on rear) (6GK5324-4QG10-3HR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/

SCALANCE XR324-4M PoE (24V, ports on front) (6GK5324-4QG10-1AR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M PoE (24V, ports on rear) (6GK5324-4QG10-1HR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XR324-4M PoE TS (24V, ports on front) (6GK5324-4QG10-1CR2): All versions < V4.1.7 affected by CVE-2022-0778	Update to V4.1.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109820827/
SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG family:	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XB-200 family:	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XB205-3 (SC, PN) (6GK5205-3BB00-2AB2): All versions < V4.4 affected by CVE-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XC-200 family:	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SIPLUS NET SCALANCE XC206-2 (6AG1206-2BB00-7AC2): All versions < V4.4 affected by CVE-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XF-200BA family:	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/

SCALANCE XP-200 family:	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XP208 (6GK5208-0HA00-2AS6): All versions < V4.4 affected by CVE-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XR-300WG family:	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	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-2022-0778	Update to V4.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817768/
SCALANCE XF201-3P IRT (6GK5201-3BH00-2BD2): All versions < V5.5.2 affected by CVE-2022-0778	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE XF202-2P IRT (6GK5202-2BH00-2BD2): All versions < V5.5.2 affected by CVE-2022-0778	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE XF204 (6GK5204-0BA00-2AF2): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE XF204-2 (6GK5204-2BC00-2AF2): All versions affected by CVE-2022-0778	Currently no fix is planned

SCALANCE XF204-2BA IRT (6GK5204-2AA00-2BD2): All versions < V5.5.2 affected by CVE-2022-0778	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE XF204IRT (6GK5204-0BA00-2BF2): All versions < V5.5.2 affected by CVE-2022-0778	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE XF206-1 (6GK5206-1BC00-2AF2): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE XF208 (6GK5208-0BA00-2AF2): All versions affected by CVE-2022-0778	Currently no fix is planned
SCALANCE XM-400/XR-500 family:	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XM-400 family:	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XM408-4C (6GK5408-4GP00-2AM2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XM408-4C (L3 int.) (6GK5408-4GQ00-2AM2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XM408-8C (6GK5408-8GS00-2AM2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XM408-8C (L3 int.) (6GK5408-8GR00-2AM2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XM416-4C (6GK5416-4GS00-2AM2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XM416-4C (L3 int.) (6GK5416-4GR00-2AM2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XR-500 family:	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/

SCALANCE XR524-8C, 1x230V (6GK5524-8GS00-3AR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XR524-8C, 1x230V (L3 int.) (6GK5524-8GR00-3AR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XR524-8C, 24V (6GK5524-8GS00-2AR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XR524-8C, 24V (L3 int.) (6GK5524-8GR00-2AR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XR524-8C, 2x230V (6GK5524-8GS00-4AR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XR524-8C, 2x230V (L3 int.) (6GK5524-8GR00-4AR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XR526-8C, 1x230V (6GK5526-8GS00-3AR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XR526-8C, 1x230V (L3 int.) (6GK5526-8GR00-3AR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XR526-8C, 24V (6GK5526-8GS00-2AR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XR526-8C, 24V (L3 int.) (6GK5526-8GR00-2AR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XR526-8C, 2x230V (6GK5526-8GS00-4AR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XR526-8C, 2x230V (L3 int.) (6GK5526-8GR00-4AR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/

SCALANCE XR528-6M (6GK5528-0AA00-2AR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XR528-6M (2HR2, L3 int.) (6GK5528-0AR00-2HR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XR528-6M (2HR2) (6GK5528-0AA00-2HR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XR528-6M (L3 int.) (6GK5528-0AR00-2AR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XR552-12M (6GK5552-0AA00-2AR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XR552-12M (2HR2, L3 int.) (6GK5552-0AR00-2AR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XR552-12M (2HR2) (6GK5552-0AA00-2HR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
SCALANCE XR552-12M (2HR2) (6GK5552-0AR00-2HR2): All versions < V6.5 affected by CVE-2022-0778	Update to V6.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109809635/
Security Configuration Tool (SCT): All versions affected by CVE-2022-0778	Currently no fix is planned
SIMATIC Cloud Connect 7 CC712 (6GK1411-1AC00): All versions < V1.9 affected by CVE-2022-0778	Update to V1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109812235/
SIMATIC Cloud Connect 7 CC716 (6GK1411-5AC00): All versions < V1.9 affected by CVE-2022-0778	Update to V1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109812235/
SIMATIC CP 343-1 Advanced (6GK7343-1GX31-0XE0): All versions affected by CVE-2022-0778	Currently no fix is planned

SIMATIC CP 443-1 Advanced (6GK7443-1GX30-0XE0): All versions < V3.3 affected by CVE-2022-0778	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109817938/
SIMATIC CP 443-1 OPC UA (6GK7443-1UX00-0XE0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIMATIC CP 1242-7 V2 (6GK7242-7KX31-0XE0): All versions < V3.4.29 affected by CVE-2022-0778	Update to V3.4.29 or later version https://support.industry.siemens.com/cs/ww/en/view/109823721/
SIMATIC CP 1243-1 (6GK7243-1BX30-0XE0): All versions < V3.4.29 affected by CVE-2022-0778	Update to V3.4.29 or later version https://support.industry.siemens.com/cs/ww/en/view/109823721/
SIMATIC CP 1243-7 LTE EU (6GK7243-7KX30-0XE0): All versions < V3.4.29 affected by CVE-2022-0778	Update to V3.4.29 or later version https://support.industry.siemens.com/cs/ww/en/view/109823721/
SIMATIC CP 1243-7 LTE US (6GK7243-7SX30-0XE0): All versions < V3.4.29 affected by CVE-2022-0778	Update to V3.4.29 or later version https://support.industry.siemens.com/cs/ww/en/view/109823721/
SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0): All versions < V3.4.29 affected by CVE-2022-0778	Update to V3.4.29 or later version https://support.industry.siemens.com/cs/ww/en/view/109823721/
SIMATIC CP 1542SP-1 (6GK7542-6UX00-0XE0): All versions < V2.2.28 affected by CVE-2022-0778	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/
SIMATIC CP 1543-1 (6GK7543-1AX00-0XE0): All versions < V3.0.37 affected by CVE-2022-0778	Update to V3.0.37 or later version https://support.industry.siemens.com/cs/ww/en/view/109828349/
SIMATIC CP 1543SP-1 (6GK7543-6WX00-0XE0): All versions < V2.2.28 affected by CVE-2022-0778	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/
SIMATIC CP 1545-1 (6GK7545-1GX00-0XE0): All versions affected by CVE-2022-0778	Currently no fix is available
SIMATIC CP 1626 (6GK1162-6AA01): All versions affected by CVE-2022-0778	Currently no fix is planned
SIMATIC CP 1628 (6GK1162-8AA00): All versions affected by CVE-2022-0778	Currently no fix is planned

SIMATIC Drive Controller CPU 1504D TF (6ES7615-4DF10-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109773914/
SIMATIC Drive Controller CPU 1507D TF (6ES7615-7DF10-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109773914/
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions < V21.9.7 affected by CVE-2022-0778	Update to V21.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109759122/
SIMATIC HMI Unified Comfort Panels: All versions < V18 affected by CVE-2022-0778	Update to V18 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530/
SIMATIC Logon V1.6: All versions < V1.6 Upd6 affected by CVE-2022-0778	Update to V1.6 Upd6 or later version https://support.industry.siemens.com/cs/ww/en/view/109805072/
SIMATIC MV540 H (6GF3540-0GE10): All versions < V3.3 affected by CVE-2022-0778	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109811878/
SIMATIC MV540 S (6GF3540-0CD10): All versions < V3.3 affected by CVE-2022-0778	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109811878/
SIMATIC MV550 H (6GF3550-0GE10): All versions < V3.3 affected by CVE-2022-0778	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109811878/
SIMATIC MV550 S (6GF3550-0CD10): All versions < V3.3 affected by CVE-2022-0778	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109811878/
SIMATIC MV560 U (6GF3560-0LE10): All versions < V3.3 affected by CVE-2022-0778	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109811878/
SIMATIC MV560 X (6GF3560-0HE10): All versions < V3.3 affected by CVE-2022-0778	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109811878/
SIMATIC NET PC Software:	See below
SIMATIC NET PC Software V14: All versions affected by CVE-2022-0778	Currently no fix is planned

SIMATIC NET PC Software V15: All versions affected by CVE-2022-0778	Currently no fix is planned
SIMATIC NET PC Software V16: All versions < V16 Update 6 affected by CVE-2022-0778	Update to V16 Update 6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811815/
SIMATIC NET PC Software V17: All versions < V17 SP1 Update 1 affected by CVE-2022-0778	Update to V17 SP1 Update 1 or later version https://support.industry.siemens.com/cs/ww/en/view/109820674/
SIMATIC PCS 7 TeleControl: All versions < V9.1 Update 1 affected by CVE-2022-0778	Update to V9.1 Update 1 or later version https://support.industry.siemens.com/cs/ww/en/view/109826159/
SIMATIC PCS 7 V8.2: All versions affected by CVE-2022-0778	Currently no fix is planned
SIMATIC PCS 7 V9.0: All versions affected by CVE-2022-0778	Currently no fix is planned
SIMATIC PCS 7 V9.1: All versions < V9.1 SP2 UC04 affected by CVE-2022-0778	Update to V9.1 SP2 UC04 or later version For the unfixed component in this version (OpenPCS 7): Restrict access to the OPC UA interface of OpenPCS 7 to trusted systems https://support.industry.siemens.com/cs/ww/en/view/109812242/
SIMATIC PCS neo (Administration Console): All versions < V4.0 affected by CVE-2022-0778	Update to V4.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109814551/
SIMATIC PDM: All versions < V9.2 SP2 affected by CVE-2022-0778	Update to V9.2 SP2 or later version https://support.industry.siemens.com/cs/ww/en/view/109811911/
SIMATIC Process Historian OPC UA Server: All versions < V2020 SP1 Update 1 affected by CVE-2022-0778	Update to V2020 SP1 Update 1 or later version In the context of SIMATIC PCS neo, update to SIMATIC PCS neo V4.0 or later version (https://support.industry.siemens.com/cs/ww/de/view/109814551/); in the context of SIMATIC PCS 7, update to SIMATIC PCS 7 V9.1 SP2 or later version (https://support.industry.siemens.com/cs/ww/en/view/109812240/); in the context of SIMATIC WinCC, contact local support
SIMATIC READER RF1xxC Family:	Update to V2.0.1 or later version https://support.industry.siemens.com/cs/de/en/view/109811120/

SIMATIC RF166C (6GT2002-0EE20): All versions < V2.0.1 affected by CVE-2022-0778	Update to V2.0.1 or later version https://support.industry.siemens.com/cs/de/en/view/109811120/
SIMATIC RF185C (6GT2002-0JE10): All versions < V2.0.1 affected by CVE-2022-0778	Update to V2.0.1 or later version https://support.industry.siemens.com/cs/de/en/view/109811120/
SIMATIC RF186C (6GT2002-0JE20): All versions < V2.0.1 affected by CVE-2022-0778	Update to V2.0.1 or later version https://support.industry.siemens.com/cs/de/en/view/109811120/
SIMATIC RF186CI (6GT2002-0JE50): All versions < V2.0.1 affected by CVE-2022-0778	Update to V2.0.1 or later version https://support.industry.siemens.com/cs/de/en/view/109811120/
SIMATIC RF188C (6GT2002-0JE40): All versions < V2.0.1 affected by CVE-2022-0778	Update to V2.0.1 or later version https://support.industry.siemens.com/cs/de/en/view/109811120/
SIMATIC RF188CI (6GT2002-0JE60): All versions < V2.0.1 affected by CVE-2022-0778	Update to V2.0.1 or later version https://support.industry.siemens.com/cs/de/en/view/109811120/
SIMATIC READER RF6xxR Family:	Update to V4.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109811014/
SIMATIC RF610R (6GT2811-6BC10): All versions < V4.0.1 affected by CVE-2022-0778	Update to V4.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109811014/
SIMATIC RF615R (6GT2811-6CC10): All versions < V4.0.1 affected by CVE-2022-0778	Update to V4.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109811014/
SIMATIC RF650R (6GT2811-6AB20): All versions < V4.0.1 affected by CVE-2022-0778	Update to V4.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109811014/
SIMATIC RF680R (6GT2811-6AA10): All versions < V4.0.1 affected by CVE-2022-0778	Update to V4.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109811014/
SIMATIC RF685R (6GT2811-6CA10): All versions < V4.0.1 affected by CVE-2022-0778	Update to V4.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109811014/

SIMATIC RF360R (6GT2801-5BA30): All versions < V2.0.1 affected by CVE-2022-0778	Update to V2.0.1 or later version https://support.industry.siemens.com/cs/de/en/view/109811118/
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions < V4.6.0 affected by CVE-2022-0778	Update to V4.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109814248/
SIMATIC S7-1500 CPU 1510SP F-1 PN (6ES7510-1SJ00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIMATIC S7-1500 CPU 1510SP F-1 PN (6ES7510-1SJ01-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1510SP-1 PN (6ES7510-1DJ00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIMATIC S7-1500 CPU 1510SP-1 PN (6ES7510-1DJ01-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AK00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AK01-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AK02-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1511C-1 PN (6ES7511-1CK00-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1511C-1 PN (6ES7511-1CK01-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FK00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned

SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FK01-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FK02-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1511T-1 PN (6ES7511-1TK01-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1511TF-1 PN (6ES7511-1UK01-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1512C-1 PN (6ES7512-1CK00-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1512C-1 PN (6ES7512-1CK01-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1512SP F-1 PN (6ES7512-1SK00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIMATIC S7-1500 CPU 1512SP F-1 PN (6ES7512-1SK01-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1512SP-1 PN (6ES7512-1DK00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIMATIC S7-1500 CPU 1512SP-1 PN (6ES7512-1DK01-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AL00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AL01-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AL02-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL01-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL02-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1513R-1 PN (6ES7513-1RL00-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM01-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM02-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM01-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM02-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1515R-2 PN (6ES7515-2RM00-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIMATIC S7-1500 CPU 1515T-2 PN (6ES7515-2TM01-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1515TF-2 PN (6ES7515-2UM01-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN01-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN02-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN00-0AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN01-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN02-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1516T-3 PN/DP (6ES7516-3TN00-0AB0): All versions < V3.0.1 affected by CVE-2022-0778	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1516TF-3 PN/DP (6ES7516-3UN00-0AB0): All versions < V3.0.1 affected by CVE-2022-0778	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1517-3 PN/DP (6ES7517-3AP00-0AB0): All versions < V3.0.1 affected by CVE-2022-0778	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1517F-3 PN/DP (6ES7517-3FP00-0AB0): All versions < V3.0.1 affected by CVE-2022-0778	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIMATIC S7-1500 CPU 1517H-3 PN (6ES7517-3HP00-0AB0): All versions < V3.0.1 affected by CVE-2022-0778	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1517T-3 PN/DP (6ES7517-3TP00-0AB0): All versions < V3.0.1 affected by CVE-2022-0778	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1517TF-3 PN/DP (6ES7517-3UP00-0AB0): All versions < V3.0.1 affected by CVE-2022-0778	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1518-4 PN/DP (6ES7518-4AP00-0AB0): All versions < V3.0.1 affected by CVE-2022-0778	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1518-4 PN/DP MFP (6ES7518-4AX00-1AB0): All versions < V3.0.1 affected by CVE-2022-0778	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1518F-4 PN/DP (6ES7518-4FP00-0AB0): All versions < V3.0.1 affected by CVE-2022-0778	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP (6ES7518-4FX00-1AB0): All versions < V3.0.1 affected by CVE-2022-0778	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1518HF-4 PN (6ES7518-4JP00-0AB0): All versions < V3.0.1 affected by CVE-2022-0778	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1518T-4 PN/DP (6ES7518-4TP00-0AB0): All versions < V3.0.1 affected by CVE-2022-0778	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1518TF-4 PN/DP (6ES7518-4UP00-0AB0): All versions < V3.0.1 affected by CVE-2022-0778	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU S7-1518-4 PN/DP ODK (6ES7518-4AP00-3AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU S7-1518F-4 PN/DP ODK (6ES7518-4FP00-3AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIMATIC S7-1500 ET 200pro: CPU 1513PRO F-2 PN (6ES7513-2GL00-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 ET 200pro: CPU 1513PRO-2 PN (6ES7513-2PL00-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 ET 200pro: CPU 1516PRO F-2 PN (6ES7516-2GN00-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 ET 200pro: CPU 1516PRO-2 PN (6ES7516-2PN00-0AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 Software Controller V2: All versions < V21.9.7 affected by CVE-2022-0778	Update to V21.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478528/
SIMATIC S7-PLCSIM Advanced: All versions < V5.0 affected by CVE-2022-0778	Update to V5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109809300/
SIMATIC STEP 7 (TIA Portal): All versions affected by CVE-2022-0778	Currently no fix is available
SIMATIC STEP 7 V5: All versions < V5.7 HF4 affected by CVE-2022-0778	Update to V5.7 HF4 or later version https://support.industry.siemens.com/cs/ww/en/view/109811212/
SIMATIC WinCC Unified (TIA Portal): All versions < V17 Update 5 affected by CVE-2022-0778	Update to V17 Update 5 or later version https://support.industry.siemens.com/cs/ww/en/view/109792171/
SIMATIC WinCC V7.3: All versions affected by CVE-2022-0778	Currently no fix is planned
SIMATIC WinCC V7.4: All versions < V7.4 SP1 Update 22 affected by CVE-2022-0778	Update to V7.4 SP1 Update 22 or later version https://support.industry.siemens.com/cs/ww/en/view/109826450/
SIMATIC WinCC V7.5: All versions < V7.5 SP2 Update 16 affected by CVE-2022-0778	Update to V7.5 SP2 Update 16 or later version https://support.industry.siemens.com/cs/ww/en/view/109793460/
SIMOTION: All versions >= V5.1 < V5.5.1 affected by CVE-2022-0778	Update to V5.5.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109812773/

SINAUT Software ST7sc: All versions affected by CVE-2022-0778	Currently no fix is planned
SINAUT ST7CC: All versions affected by CVE-2022-0778	Currently no fix is planned
SINEC INS: All versions < V1.0 SP2 affected by CVE-2022-0778	Update to V1.0 SP2 or later version https://support.industry.siemens.com/cs/ww/en/view/109812610/
SINEC NMS: All versions < V1.0 SP3 affected by CVE-2022-0778	Update to V1.0 SP3 or later version https://support.industry.siemens.com/cs/ww/en/view/109813788/
SINEMA Remote Connect Server: All versions < V3.1 affected by CVE-2022-0778	Update to V3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109811169/
SIPLUS ET 200SP CP 1543SP-1 ISEC (6AG1543-6WX00-7XE0): All versions < V2.2.28 affected by CVE-2022-0778	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/
SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (6AG2543-6WX00-4XE0): All versions < V2.2.28 affected by CVE-2022-0778	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/
SIPLUS ET 200SP CPU 1510SP F-1 PN (6AG1510-1SJ01-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1510SP F-1 PN RAIL (6AG2510-1SJ01-1AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1510SP-1 PN (6AG1510-1DJ01-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1510SP-1 PN (6AG1510-1DJ01-7AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1510SP-1 PN RAIL (6AG2510-1DJ01-1AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1510SP-1 PN RAIL (6AG2510-1DJ01-4AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIPLUS ET 200SP CPU 1512SP F-1 PN (6AG1512-1SK00-2AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIPLUS ET 200SP CPU 1512SP F-1 PN (6AG1512-1SK01-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1512SP F-1 PN (6AG1512-1SK01-7AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1512SP F-1 PN RAIL (6AG2512-1SK01-1AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1512SP F-1 PN RAIL (6AG2512-1SK01-4AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1512SP-1 PN (6AG1512-1DK01-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1512SP-1 PN (6AG1512-1DK01-7AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1512SP-1 PN RAIL (6AG2512-1DK01-1AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1512SP-1 PN RAIL (6AG2512-1DK01-4AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS NET CP 343-1 Advanced (6AG1343-1GX31-4XE0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIPLUS NET CP 443-1 Advanced (6AG1443-1GX30-4XE0): All versions < V3.3 affected by CVE-2022-0778	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109817938/
SIPLUS NET CP 1242-7 V2 (6AG1242-7KX31-7XE0): All versions < V3.4.29 affected by CVE-2022-0778	Update to V3.4.29 or later version https://support.industry.siemens.com/cs/ww/en/view/109823721/

SIPLUS NET CP 1543-1 (6AG1543-1AX00-2XE0): All versions < V3.0.37 affected by CVE-2022-0778	Update to V3.0.37 or later version https://support.industry.siemens.com/cs/ww/en/view/109828349/
SIPLUS NET SCALANCE X202-2P IRT (6AG1202-2BH00-2BA3): All versions < V5.5.2 affected by CVE-2022-0778	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SIPLUS S7-1200 CP 1243-1 (6AG1243-1BX30-2AX0): All versions < V3.4.29 affected by CVE-2022-0778	Update to V3.4.29 or later version https://support.industry.siemens.com/cs/ww/en/view/109823721/
SIPLUS S7-1200 CP 1243-1 RAIL (6AG2243-1BX30-1XE0): All versions < V3.4.29 affected by CVE-2022-0778	Update to V3.4.29 or later version https://support.industry.siemens.com/cs/ww/en/view/109823721/
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK00-2AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK01-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK01-7AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK02-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK02-7AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1511-1 PN T1 RAIL (6AG2511-1AK01-1AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1511-1 PN T1 RAIL (6AG2511-1AK02-1AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1511-1 PN TX RAIL (6AG2511-1AK01-4AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIPLUS S7-1500 CPU 1511-1 PN TX RAIL (6AG2511-1AK02-4AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1511F-1 PN (6AG1511-1FK00-2AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIPLUS S7-1500 CPU 1511F-1 PN (6AG1511-1FK01-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1511F-1 PN (6AG1511-1FK02-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL00-2AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL01-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL01-7AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL02-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL02-7AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1513F-1 PN (6AG1513-1FL00-2AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIPLUS S7-1500 CPU 1513F-1 PN (6AG1513-1FL01-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1513F-1 PN (6AG1513-1FL02-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIPLUS S7-1500 CPU 1515F-2 PN (6AG1515-2FM01-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1515F-2 PN (6AG1515-2FM02-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1515F-2 PN RAIL (6AG2515-2FM02-4AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1515F-2 PN T2 RAIL (6AG2515-2FM01-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1515R-2 PN (6AG1515-2RM00-7AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1515R-2 PN TX RAIL (6AG2515-2RM00-4AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN00-2AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN00-7AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN01-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN01-7AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN02-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN02-7AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIPLUS S7-1500 CPU 1516-3 PN/DP RAIL (6AG2516-3AN02-4AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1516-3 PN/DP TX RAIL (6AG2516-3AN01-4AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1516F-3 PN/DP (6AG1516-3FN00-2AB0): All versions affected by CVE-2022-0778	Currently no fix is planned
SIPLUS S7-1500 CPU 1516F-3 PN/DP (6AG1516-3FN01-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1516F-3 PN/DP (6AG1516-3FN02-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1516F-3 PN/DP RAIL (6AG2516-3FN02-2AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1516F-3 PN/DP RAIL (6AG2516-3FN02-4AB0): All versions < V2.9.7 affected by CVE-2022-0778	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1517H-3 PN (6AG1517-3HP00-4AB0): All versions < V3.0.1 affected by CVE-2022-0778	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1518-4 PN/DP (6AG1518-4AP00-4AB0): All versions < V3.0.1 affected by CVE-2022-0778	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1518-4 PN/DP MFP (6AG1518-4AX00-4AC0): All versions < V3.0.1 affected by CVE-2022-0778	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1518F-4 PN/DP (6AG1518-4FP00-4AB0): All versions < V3.0.1 affected by CVE-2022-0778	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1518HF-4 PN (6AG1518-4JP00-4AB0): All versions < V3.0.1 affected by CVE-2022-0778	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0): All versions < V2.4.8 affected by CVE-2022-0778	Update to V2.4.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109954889/
TeleControl Server Basic V3: All versions < V3.1.1 affected by CVE-2022-0778	Update to V3.1.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109812231/
TIA Administrator: All versions < V1.0 SP8 affected by CVE-2022-0778	Update to V1.0 SP8 or later version https://support.industry.siemens.com/cs/ww/en/view/114358/
TIM 1531 IRC (6GK7543-1MX00-0XE0): All versions < V2.4.8 affected by CVE-2022-0778	Update to V2.4.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109954889/
Totally Integrated Automation Portal (TIA Portal):	See below
Totally Integrated Automation Portal (TIA Portal) V15: All versions affected by CVE-2022-0778	Currently no fix is planned
Totally Integrated Automation Portal (TIA Portal) V16: All versions affected by CVE-2022-0778	Currently no fix is planned
Totally Integrated Automation Portal (TIA Portal) V17: All versions < V17 Update 5 affected by CVE-2022-0778	Update to V17 Update 5 or later version https://support.industry.siemens.com/cs/ww/en/view/109784441/

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

SIMATIC CP 1623, CP 1626 and CP 1628 are PCI express cards for connection to Industrial Ethernet.

Industrial Edge represents an open, ready-to-use Edge computing platform consisting of Edge devices, Edge apps, Edge connectivity, and an application and device management infrastructure.

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.

SIMATIC RF600 Readers are used for the contactless identification of every kind of object, e.g. transport containers, pallets, production goods, or it can be generally used for recording goods in bulk.

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 LPE9000 (Local Processing Engine) extends the SCALANCE family portfolio by a component that provides computing power for a wide range of applications in the network, close to the process – Edge Computing.

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 W1750D is an Access Point that supports IEEE 802.11ac standards for high-performance WLAN, and is equipped with two dual-band radios, which can provide access and monitor the network simultaneously.

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).

Security Configuration Tool (SCT) is an engineering software for security devices such as SCALANCE-S or CP 443-1 Advanced.

SIMATIC Cloud Connect 7 is an IoT Gateway to connect programmable logic controllers to cloud services and enables the connection of field devices with OPC UA server Interface as OPC UA clients.

SIMATIC CP 1242-7 and CP 1243-7 LTE communications processors connect SIMATIC S7-1200 controllers to Wide Area Networks (WAN). They provide integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

SIMATIC CP 1243-8 IRC communications processors connect SIMATIC S7-1200 controllers via the SINAUT ST7 telecontrol protocol to a control center or master ST7 stations.

SIMATIC CP 1243-1 communications processors connect S7-1200 controllers to Ethernet networks. They provide integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

SIMATIC CP 1543-1, CP 1543SP-1, CP 1542SP-1 and CP 1542SP-1 IRC communications processors connect SIMATIC S7-1500 controllers to Ethernet networks. They provide integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

SIMATIC CP 343-1 and CP 443-1 are communication processors (CP) designed to enable Ethernet communication for SIMATIC S7-300/S7-400 CPUs.

SIMATIC Drive Controllers have been designed for the automation of production machines, combining the functionality of a SIMATIC S7-1500 CPU and a SINAMICS S120 drive control.

SIMATIC ET 200SP Open Controller is a PC-based version of the SIMATIC S7-1500 Controller including optional visualization in combination with central I/Os in a compact device.

SIMATIC HMI Panels are used for operator control and monitoring of machines and plants.

SIMATIC Logon is used for central user administration and access control in other SIMATIC applications.

SIMATIC MV500 products are stationary optical readers, used to reliably capture printed, lasered, drilled, punched and dotpeen codes on a variety of different surfaces.

SIMATIC NET PC software is a software product that is sold separately and implements the communications product from SIMATIC NET.

SIMATIC PCS 7 is a distributed control system (DCS) integrating SIMATIC WinCC, SIMATIC Batch, SIMATIC Route Control, OpenPCS 7 and other components.

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

SIMATIC PDM (Process Device Manager) is an universal, manufacturer-independent tool for configuration, parameter assignment, commissioning, diagnostics and maintenance of intelligent process devices (actors, sensors) and automation components (remote I/Os, multiplexer, process control units, compact controller).

SIMATIC RF180C is an RFID communication module for direct connection of SIMATIC identification systems to PROFINET IO/Ethernet. SIMATIC RF180C is superseded by the SIMATIC RF18xC devices (RF185C, RF186C, RF188C).

The SIMATIC RF360R reader extends the SIMATIC RF300 RFID system by a compact reader with an integrated Industrial Ethernet interface.

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

SIMATIC S7-1500 CPU products have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIMATIC S7-1500 Software Controller is a SIMATIC software controller for PC-based automation solutions.

SIMATIC S7-PLCSIM Advanced simulates S7-1200, S7-1500 and a few other PLC derivatives. Includes full network access to simulate the PLCs, even in virtualized environments.

SIMATIC STEP 7 (TIA Portal) is an engineering software to configure and program SIMATIC controllers.

SIMATIC STEP 7 V5 is the classic engineering software to configure and program SIMATIC S7-300/S7-400/C7/WinAC controllers.

SIMATIC WinCC is a supervisory control and data acquisition (SCADA) system.

SIMATIC WinCC Unified is a completely new visualization system that enables you to successfully master the challenges of digitization in machine and plant engineering.

SIMOTION is a scalable high performance hardware and software system for motion control.

SINAUT Software ST7sc connects SINAUT ST7 stations to HMI, SCADA and office applications via OPC.

SINAUT ST7CC allows remote monitoring and control of plants.

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.

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.

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.

TeleControl Server Basic allows remote monitoring and control of plants.

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.

Totally Integrated Automation Portal (TIA Portal) is a PC software that provides access to the complete range of Siemens digitalized automation services, from digital planning and integrated engineering to transparent operation.

TIM 1531 IRC is a communication module for SIMATIC S7-1500, S7-400, S7-300 with SINAUT ST7, DNP3 and IEC 60870-5-101/104 with three RJ45 interfaces for communication via IP-based networks (WAN / LAN) and a RS 232/RS 485 interface for communication via classic WAN 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-2022-0778

The BN_mod_sqrt() function in openSSL, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')

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 (2022-06-14): Publication Date

V1.1 (2022-07-12): Added SCALANCE X-200, X-200 IRT, X-300, XM-400, XR-500, XR-300WG, XB-200, XC-200, XF-200, XP-200 product families and Security Configuration Tool (SCT) as affected; added fix for RUGGEDCOM ROX devices and SIMATIC MV500 devices; no fix planned for SIMATIC NET PC Software, SIMATIC CP 343-1 Advanced and SIMATIC CP 443-1 Advanced (incl. SIPLUS NET variants)

V1.2 (2022-08-09): Added fix for Industrial Edge - OPC UA Connector, SIMATIC Cloud Connect 7 gateways, SIMATIC Logon, SIMATIC PDM, SIMATIC STEP 7 V5.X and TeleControl Server Basic; added SCALANCE W1750D as affected; clarified that Industrial Edge - PROFINET IO Connector is not affected

V1.3 (2022-09-13): Added fix for RUGGEDCOM CROSSBOW Station Access Controller (SAC), SCALANCE XM-400 and XR-500 product families, and SINEC INS

V1.4 (2022-10-11): Added fix for SIMATIC WinCC Unified, TIA Portal V17, and SINEC NMS; added SCALANCE W-700 and W-1700 product families as affected; corrected several product names in the SCALANCE XB and XP product families

V1.5 (2022-12-13): Added SIMATIC Process Historian and SIMATIC HMI Unified Comfort Panels; added fix for SIMATIC PCS neo, SIMATIC Drive Controller family, SIMATIC S7-PLCSIM Advanced, SIMATIC S7-1500 and S7-1200 CPU families, and TIA Administrator; no fix planned for TIA Portal V16

V1.6 (2023-01-10): Added fix for SCALANCE W-700 IEEE 802.11ax product family

V1.7 (2023-02-14): Added fix for SCALANCE W1750D product family

V1.8 (2023-03-14): Added fix for SIMATIC CP 1542SP-1 and SIMATIC CP 1543SP-1, RUGGEDCOM RM1224 family, SCALANCE M-800 family, SCALANCE MUM-800 family, SCALANCE S615. Added missing affected products SCALANCE M876-4 (6GK5876-4AA10-2BA2) and SCALANCE S615 EEC (6GK5615-0AA01- 2AA2)

V1.9 (2023-04-11): Added fix for SCALANCE X-200IRT family, SIMATIC CP 443-1 Advanced, TIM 1531 IRC, SCALANCE XB-200, XC-200, XP-200, XF-200BA, XR-300WG family, and for SIMATIC WinCC

V2.0 (2023-05-09): Added fix for SIMATIC S7-1500 Software Controller; fix planned for SIMATIC NET PC Software V17

V2.1 (2023-06-13): Added fix for SIMOTION; clarified that no fix is planned for V8.2, V9.0, V9.1 of OpenPCS 7 and for V8.2, V9.0 of SIMATIC PCS 7; added fix and mitigation information for SIMATIC PCS 7 V9.1

V2.2 (2023-07-11): Expanded SIMATIC S7-1500 CPU family to individual products/MLFBs and added additional fix for V2 firmware version line; Fix for SIMATIC Drive Controller available already with V2.9.7

V2.3 (2023-09-12): Clarified SIMATIC S7-1500 Software Controller versions and adjusted fix for SIMATIC S7-1500 Software Controller V2; Clarified SIMATIC ET 200SP Open Controller versions and added fix for SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants)

V2.4 (2023-10-10): Added fix for SIMATIC CP 1242-7 V2 family, SIMATIC CP 1243-1 family, SIMATIC CP 1243-7 LTE family, SIMATIC CP 1243-8 IRC and for SIMATIC NET PC Software V17

V2.5 (2024-01-09): Added fix for SIMATIC PCS 7 TeleControl; Clarified that no fix is planned for SINAUT Software ST7sc and SINAUT ST7CC

V2.6 (2024-04-09): Added fix for SIMATIC CP 1543-1 (incl. SIPLUS variants); Updated fix for TIM 1531 IRC (incl. SIPLUS NET variants)

V2.7 (2024-05-14): Expanded SIMATIC WinCC family to individual version lines; SIMATIC PCS 7 V9.1: clarified that V9.1 SP2 UC04 fixes the issue in SIMATIC WinCC

V2.8 (2024-07-09): Added fix for SCALANCE X-300 family (incl. X408 and SIPLUS NET variants)

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.