SSA-780073: Denial of Service Vulnerability in PROFINET Devices via DCE-RPC Packets

Publication Date: 2020-02-11
Last Update: 2024-07-09
Current Version: V2.4
CVSS v3.1 Base Score: 7.5

SUMMARY

Products that include the Siemens PROFINET-IO (PNIO) stack in versions prior V06.00 are potentially affected by a denial of service vulnerability when multiple legitimate diagnostic package requests are sent to the DCE-RPC interface.

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

Additionally, Siemens recommends other vendors of PROFINET devices to check if their products have incorporated a vulnerable version of the Siemens PNIO stack as part of the Siemens Development/Evaluation Kits.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller: All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200: All Versions < V4.5 affected by CVE-2019-13946	Update to V4.5 Patch 01 https://support.industry.siemens.com/cs/ww/en/view/109760397/ See further recommendations from section Workarounds and Mitigations
Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P: All Versions < V4.6 affected by CVE-2019-13946	Update to V4.6 https://support.industry.siemens.com/cs/ww/en/view/109765183/ See further recommendations from section Workarounds and Mitigations
PROFINET Driver for Controller: All Versions < V2.1 affected by CVE-2019-13946	Update to V2.1 Patch 03 https://support.industry.siemens.com/cs/ww/en/view/109768047/ See further recommendations from section Workarounds and Mitigations

SCALANCE M-800 family (incl. S615, MUM-800 and RM1224):	Update to V6.1.2 or later version Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp) https://support.industry.siemens.com/cs/ww/en/view/109772130/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RM1224 family (6GK6108-4AM00): All versions < V4.3 affected by CVE-2019-13946	Update to V6.1.2 or later version Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp) https://support.industry.siemens.com/cs/ww/en/view/109772130/ See further recommendations from section Workarounds and Mitigations
SCALANCE M-800 family:	Update to V6.1.2 or later version Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp) https://support.industry.siemens.com/cs/ww/en/view/109772130/ See further recommendations from section Workarounds and Mitigations
SCALANCE M804PB (6GK5804-0AP00-2AA2): All versions < V4.3 affected by CVE-2019-13946	Update to V6.1.2 or later version Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp) https://support.industry.siemens.com/cs/ww/en/view/109772130/ See further recommendations from section Workarounds and Mitigations
SCALANCE M812-1 ADSL-Router family:	Update to V6.1.2 or later version Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp) https://support.industry.siemens.com/cs/ww/en/view/109772130/ See further recommendations from section Workarounds and Mitigations
SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2): All versions < V4.3 affected by CVE-2019-13946	Update to V6.1.2 or later version Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp) https://support.industry.siemens.com/cs/ww/en/view/109772130/ See further recommendations from section Workarounds and Mitigations

SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2): All versions < V4.3 affected by CVE-2019-13946	Update to V6.1.2 or later version Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp) https://support.industry.siemens.com/cs/ww/en/view/109772130/ See further recommendations from section Workarounds and Mitigations
SCALANCE M816-1 ADSL-Router family:	Update to V6.1.2 or later version Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp) https://support.industry.siemens.com/cs/ww/en/view/109772130/ See further recommendations from section Workarounds and Mitigations
SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2): All versions < V4.3 affected by CVE-2019-13946	Update to V6.1.2 or later version Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp) https://support.industry.siemens.com/cs/ww/en/view/109772130/ See further recommendations from section Workarounds and Mitigations
SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2): All versions < V4.3 affected by CVE-2019-13946	Update to V6.1.2 or later version Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp) https://support.industry.siemens.com/cs/ww/en/view/109772130/ See further recommendations from section Workarounds and Mitigations
SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2): All versions < V4.3 affected by CVE-2019-13946	Update to V6.1.2 or later version Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp) https://support.industry.siemens.com/cs/ww/en/view/109772130/ See further recommendations from section Workarounds and Mitigations
SCALANCE M874-2 (6GK5874-2AA00-2AA2): All versions < V4.3 affected by CVE-2019-13946	Update to V6.1.2 or later version Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp) https://support.industry.siemens.com/cs/ww/en/view/109772130/ See further recommendations from section Workarounds and Mitigations

SCALANCE M874-3 (6GK5874-3AA00-2AA2): All versions < V4.3 affected by CVE-2019-13946	Update to V6.1.2 or later version Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp) https://support.industry.siemens.com/cs/ww/en/view/109772130/ See further recommendations from section Workarounds and Mitigations
SCALANCE M876-3 (6GK5876-3AA02-2BA2): All versions < V4.3 affected by CVE-2019-13946	Update to V6.1.2 or later version Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp) https://support.industry.siemens.com/cs/ww/en/view/109772130/ See further recommendations from section Workarounds and Mitigations
SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2): All versions < V4.3 affected by CVE-2019-13946	Update to V6.1.2 or later version Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp) https://support.industry.siemens.com/cs/ww/en/view/109772130/ See further recommendations from section Workarounds and Mitigations
SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2): All versions < V4.3 affected by CVE-2019-13946	Update to V6.1.2 or later version Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp) https://support.industry.siemens.com/cs/ww/en/view/109772130/ See further recommendations from section Workarounds and Mitigations
SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2): All versions < V4.3 affected by CVE-2019-13946	Update to V6.1.2 or later version Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp) https://support.industry.siemens.com/cs/ww/en/view/109772130/ See further recommendations from section Workarounds and Mitigations
SCALANCE S615 family:	Update to V6.1.2 or later version Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp) https://support.industry.siemens.com/cs/ww/en/view/109772130/ See further recommendations from section Workarounds and Mitigations

SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2): All versions < V4.3 affected by CVE-2019-13946	Update to V6.1.2 or later version Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp) https://support.industry.siemens.com/cs/ww/en/view/109772130/ See further recommendations from section Workarounds and Mitigations
SCALANCE W-700 IEEE 802.11n family: All versions <= V6.0.1 affected by CVE-2019-13946	Update to V6.4 https://support.industry.siemens.com/cs/ww/en/view/109773308/ See further recommendations from section Workarounds and Mitigations
SCALANCE X200-4P IRT (6GK5200-4AH00-2BA3): All Versions < V5.3 affected by CVE-2019-13946	Update to V5.4.2 https://support.industry.siemens.com/cs/ww/en/view/109763309/ See further recommendations from section Workarounds and Mitigations
SCALANCE X201-3P IRT (6GK5201-3BH00-2BA3): All Versions < V5.3 affected by CVE-2019-13946	Update to V5.4.2 https://support.industry.siemens.com/cs/ww/en/view/109763309/ See further recommendations from section Workarounds and Mitigations
SCALANCE X201-3P IRT PRO (6GK5201-3JR00-2BA6): All Versions < V5.3 affected by CVE-2019-13946	Update to V5.4.2 https://support.industry.siemens.com/cs/ww/en/view/109763309/ See further recommendations from section Workarounds and Mitigations
SCALANCE X202-2IRT (6GK5202-2BB00-2BA3): All Versions < V5.3 affected by CVE-2019-13946	Update to V5.4.2 https://support.industry.siemens.com/cs/ww/en/view/109763309/ See further recommendations from section Workarounds and Mitigations
SCALANCE X202-2P IRT (6GK5202-2BH00-2BA3): All Versions < V5.3 affected by CVE-2019-13946	Update to V5.4.2 https://support.industry.siemens.com/cs/ww/en/view/109763309/ See further recommendations from section Workarounds and Mitigations
SCALANCE X202-2P IRT PRO (6GK5202-2JR00-2BA6): All Versions < V5.3 affected by CVE-2019-13946	Update to V5.4.2 https://support.industry.siemens.com/cs/ww/en/view/109763309/ See further recommendations from section Workarounds and Mitigations

SCALANCE X204-2 (6GK5204-2BB10-2AA3): All versions < V5.2.5 affected by CVE-2019-13946	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204-2FM (6GK5204-2BB11-2AA3): All versions < V5.2.5 affected by CVE-2019-13946	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204-2LD (6GK5204-2BC10-2AA3): All versions < V5.2.5 affected by CVE-2019-13946	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204-2LD TS (6GK5204-2BC10-2CA2): All versions < V5.2.5 affected by CVE-2019-13946	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204-2TS (6GK5204-2BB10-2CA2): All versions < V5.2.5 affected by CVE-2019-13946	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204IRT (6GK5204-0BA00-2BA3): All Versions < V5.3 affected by CVE-2019-13946	Update to V5.4.2 https://support.industry.siemens.com/cs/ww/en/view/109763309/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204IRT PRO (6GK5204-0JA00-2BA6): All Versions < V5.3 affected by CVE-2019-13946	Update to V5.4.2 https://support.industry.siemens.com/cs/ww/en/view/109763309/ See further recommendations from section Workarounds and Mitigations
SCALANCE X206-1 (6GK5206-1BB10-2AA3): All versions < V5.2.5 affected by CVE-2019-13946	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/ See further recommendations from section Workarounds and Mitigations

SCALANCE X206-1LD (6GK5206-1BC10-2AA3): All versions < V5.2.5 affected by CVE-2019-13946	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/ See further recommendations from section Workarounds and Mitigations
SCALANCE X208 (6GK5208-0BA10-2AA3): All versions < V5.2.5 affected by CVE-2019-13946	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/ See further recommendations from section Workarounds and Mitigations
SCALANCE X208PRO (6GK5208-0HA10-2AA6): All versions < V5.2.5 affected by CVE-2019-13946	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/ See further recommendations from section Workarounds and Mitigations
SCALANCE X212-2 (6GK5212-2BB00-2AA3): All versions < V5.2.5 affected by CVE-2019-13946	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/ See further recommendations from section Workarounds and Mitigations
SCALANCE X212-2LD (6GK5212-2BC00-2AA3): All versions < V5.2.5 affected by CVE-2019-13946	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/ See further recommendations from section Workarounds and Mitigations
SCALANCE X216 (6GK5216-0BA00-2AA3): All versions < V5.2.5 affected by CVE-2019-13946	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/ See further recommendations from section Workarounds and Mitigations
SCALANCE X224 (6GK5224-0BA00-2AA3): All versions < V5.2.5 affected by CVE-2019-13946	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/ See further recommendations from section Workarounds and Mitigations
SCALANCE X-300 family (incl. X408 and SIPLUS NET variants):	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

SCALANCE X-300 EEC family:	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (230V, coated) (6GK5302-7GD00-3GA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (230V) (6GK5302-7GD00-3EA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (24V, coated) (6GK5302-7GD00-1GA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (24V) (6GK5302-7GD00-1EA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (2x 230V, coated) (6GK5302-7GD00-4GA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (2x 230V) (6GK5302-7GD00-4EA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (2x 24V, coated) (6GK5302-7GD00-2GA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

SCALANCE X302-7 EEC (2x 24V) (6GK5302-7GD00-2EA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (230V, coated) (6GK5307-2FD00-3GA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (230V) (6GK5307-2FD00-3EA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (24V, coated) (6GK5307-2FD00-1GA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (24V) (6GK5307-2FD00-1EA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (2x 230V, coated) (6GK5307-2FD00-4GA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (2x 230V) (6GK5307-2FD00-4EA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (2x 24V, coated) (6GK5307-2FD00-2GA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

SCALANCE X307-2 EEC (2x 24V) (6GK5307-2FD00-2EA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X-300 family:	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X304-2FE (6GK5304-2BD00-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X306-1LD FE (6GK5306-1BF00-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X320-1 FE (6GK5320-1BD00-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X320-1-2LD FE (6GK5320-3BF00-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X300 family:	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-3 (6GK5307-3BL00-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

SCALANCE X307-3LD (6GK5307-3BM00-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2 (6GK5308-2FL00-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LD (6GK5308-2FM00-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH (6GK5308-2FN00-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH+ (6GK5308-2FP00-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X310 (6GK5310-0FA00-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X310FE (6GK5310-0BA00-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X-300 RD family:	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

SCALANCE X307-3 (6GK5307-3BL10-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-3LD (6GK5307-3BM10-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2 RD (inkl. SIPLUS variants):	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2 (6GK5308-2FL10-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SIPLUS NET SCALANCE X308-2 (6AG1308-2FL10-4AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LD (6GK5308-2FM10-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH (6GK5308-2FN10-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH+ (6GK5308-2FP10-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

SCALANCE X310 (6GK5310-0FA10-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X310FE (6GK5310-0BA10-2AA3): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M family:	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M (6GK5308-2GG00-2AA2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M PoE (6GK5308-2QG00-2AA2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M TS (6GK5308-2GG00-2CA2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M RD family:	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M (6GK5308-2GG10-2AA2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

SCALANCE X308-2M PoE (6GK5308-2QG10-2AA2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M TS (6GK5308-2GG10-2CA2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X408 family:	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE X408-2 (6GK5408-2FD00-2AA2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR-300 family:	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (230V, ports on front) (6GK5324-0GG00-3AR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (230V, ports on rear) (6GK5324-0GG00-3HR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (24V, ports on front) (6GK5324-0GG00-1AR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR324-12M (24V, ports on rear) (6GK5324-0GG00-1HR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M TS (24V) (6GK5324-0GG00-1CR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR-300 RD family:	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (230V, ports on front) (6GK5324-0GG10-3AR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (230V, ports on rear) (6GK5324-0GG10-3HR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (24V, ports on front) (6GK5324-0GG10-1AR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (24V, ports on rear) (6GK5324-0GG10-1HR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M TS (24V) (6GK5324-0GG10-1CR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR-300 EEC family:	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front) (6GK5324-4GG00-3ER2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG00-3JR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (24V, ports on front) (6GK5324-4GG00-1ER2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (24V, ports on rear) (6GK5324-4GG00-1JR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front) (6GK5324-4GG00-4ER2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG00-4JR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 24V, ports on front) (6GK5324-4GG00-2ER2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR324-4M EEC (2x 24V, ports on rear) (6GK5324-4GG00-2JR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR-300 EEC RD family:	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front) (6GK5324-4GG10-3ER2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG10-3JR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (24V, ports on front) (6GK5324-4GG10-1ER2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (24V, ports on rear) (6GK5324-4GG10-1JR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front) (6GK5324-4GG10-4ER2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG10-4JR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR324-4M EEC (2x 24V, ports on front) (6GK5324-4GG10-2ER2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 24V, ports on rear) (6GK5324-4GG10-2JR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR-300 POE family:	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE (230V, ports on front) (6GK5324-4QG00-3AR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE (230V, ports on rear) (6GK5324-4QG00-3HR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE (24V, ports on front) (6GK5324-4QG00-1AR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE (24V, ports on rear) (6GK5324-4QG00-1HR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE TS (24V, ports on front) (6GK5324-4QG00-1CR2): All versions < V4.1.4 affected by CVE-2019-13946	Update to V4.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109808359/ See further recommendations from section Workarounds and Mitigations

SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG family:	Update to V4.1 https://support.industry.siemens.com/cs/ww/en/view/109762982/ See further recommendations from section Workarounds and Mitigations
SCALANCE XB-200 family: All Versions < V3.0 affected by CVE-2019-13946	Update to V4.1 https://support.industry.siemens.com/cs/ww/en/view/109762982/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR-300WG family: All Versions < V3.0 affected by CVE-2019-13946	Update to V4.1 https://support.industry.siemens.com/cs/ww/en/view/109762982/ See further recommendations from section Workarounds and Mitigations
SCALANCE XC-200: All Versions < V3.0 affected by CVE-2019-13946	Update to V4.1 https://support.industry.siemens.com/cs/ww/en/view/109762982/ See further recommendations from section Workarounds and Mitigations
SCALANCE XF201-3P IRT (6GK5201-3BH00-2BD2): All Versions < V5.3 affected by CVE-2019-13946	Update to V5.4.2 https://support.industry.siemens.com/cs/ww/en/view/109763309/ See further recommendations from section Workarounds and Mitigations
SCALANCE XF202-2P IRT (6GK5202-2BH00-2BD2): All Versions < V5.3 affected by CVE-2019-13946	Update to V5.4.2 https://support.industry.siemens.com/cs/ww/en/view/109763309/ See further recommendations from section Workarounds and Mitigations
SCALANCE XF204 (6GK5204-0BA00-2AF2): All versions < V5.2.5 affected by CVE-2019-13946	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/ See further recommendations from section Workarounds and Mitigations
SCALANCE XF204-2 (6GK5204-2BC00-2AF2): All versions < V5.2.5 affected by CVE-2019-13946	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/ See further recommendations from section Workarounds and Mitigations

SCALANCE XF204-2BA IRT (6GK5204-2AA00-2BD2): All Versions < V5.3 affected by CVE-2019-13946	Update to V5.4.2 https://support.industry.siemens.com/cs/ww/en/view/109763309/ See further recommendations from section Workarounds and Mitigations
SCALANCE XF204IRT (6GK5204-0BA00-2BF2): All Versions < V5.3 affected by CVE-2019-13946	Update to V5.4.2 https://support.industry.siemens.com/cs/ww/en/view/109763309/ See further recommendations from section Workarounds and Mitigations
SCALANCE XF206-1 (6GK5206-1BC00-2AF2): All versions < V5.2.5 affected by CVE-2019-13946	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/ See further recommendations from section Workarounds and Mitigations
SCALANCE XF208 (6GK5208-0BA00-2AF2): All versions < V5.2.5 affected by CVE-2019-13946	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/ See further recommendations from section Workarounds and Mitigations
SCALANCE XF-200BA: All Versions < V3.0 affected by CVE-2019-13946	Update to V4.1 https://support.industry.siemens.com/cs/ww/en/view/109762982/ See further recommendations from section Workarounds and Mitigations
SCALANCE XM-400/XR-500 family:	Update to V6.2.3 See further recommendations from section Workarounds and Mitigations
SCALANCE XM-400 family: All Versions < V6.0 affected by CVE-2019-13946	Update to V6.2.3 https://support.industry.siemens.com/cs/ww/en/view/109771191/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR-500 family: All Versions < V6.0 affected by CVE-2019-13946	Update to V6.2.3 https://support.industry.siemens.com/cs/ww/en/view/109771193/ See further recommendations from section Workarounds and Mitigations
SCALANCE XP-200: All Versions < V3.0 affected by CVE-2019-13946	Update to V4.1 https://support.industry.siemens.com/cs/ww/en/view/109762982/ See further recommendations from section Workarounds and Mitigations

SIMATIC CP 343-1 (6GK7343-1EX30-0XE0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 343-1 Advanced (6GK7343-1GX31-0XE0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 343-1 ERPC (6GK7343-1FX00-0XE0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 343-1 Lean (6GK7343-1CX10-0XE0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 (6GK7443-1EX30-0XE0): All versions < V3.3 affected by CVE-2019-13946	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109817938/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 (6GK7443-1EX30-0XE1): All versions < V3.3 affected by CVE-2019-13946	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109817938/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 Advanced (6GK7443-1GX30-0XE0): All versions < V3.3 affected by CVE-2019-13946	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109817938/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 OPC UA (6GK7443-1UX00-0XE0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 1616 and CP 1604: All Versions < V2.8 affected by CVE-2019-13946	Update to V2.8.1 https://support.industry.siemens.com/cs/ww/en/view/109768663/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 4AO U/I 4xM12 (6ES7145-6HD00-0AB0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC ET200ecoPN, 8 DIO, DC24V/1,3A, 8xM12 (6ES7147-6BG00-0AB0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8 DO, DC24V/2A, 8xM12 (6ES7142-6BR00-0AB0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8AI RTD/TC 8xM12 (6ES7144-6KD50-0AB0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8AI; 4 U/I; 4 RTD/TC 8xM12 (6ES7144-6KD00-0AB0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8DI, DC24V, 4xM12 (6ES7141-6BF00-0AB0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8DI, DC24V, 8xM12 (6ES7141-6BG00-0AB0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8DO, DC24V/0,5A, 4xM12 (6ES7142-6BF50-0AB0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8DO, DC24V/1,3A, 4xM12 (6ES7142-6BF00-0AB0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8DO, DC24V/1,3A, 8xM12 (6ES7142-6BG00-0AB0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 16DI, DC24V, 8xM12 (6ES7141-6BH00-0AB0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 16DO DC24V/1,3A, 8xM12 (6ES7142-6BH00-0AB0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN: IO-Link Master (6ES7148-6JA00-0AB0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC ET200S (incl. SIPLUS variants): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200AL IM 157-1 PN (6ES7157-1AB00-0AB0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200M IM 153-4 PN IO HF (incl. SIPLUS variants): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200M IM 153-4 PN IO ST (incl. SIPLUS variants): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200MP IM 155-5 PN HF (incl. SIPLUS variants):	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/93012181/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200MP IM 155-5 PN HF (6ES7155-5AA00-0AC0): All versions < V4.2.0 affected by CVE-2019-13946	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/93012181/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200MP IM 155-5 PN HF (6AG1155-5AA00-2AC0): All versions < V4.2.0 affected by CVE-2019-13946	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/93012181/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200MP IM 155-5 PN HF (6AG1155-5AA00-7AC0): All versions < V4.2.0 affected by CVE-2019-13946	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/93012181/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200MP IM 155-5 PN HF T1 RAIL (6AG2155-5AA00-1AC0): All versions < V4.2.0 affected by CVE-2019-13946	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/93012181/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200MP IM 155-5 PN ST (incl. SIPLUS variants):	Update to V4.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/78647504/ See further recommendations from section Workarounds and Mitigations

SIMATIC ET 200MP IM 155-5 PN ST (-Ax00) (incl. SIPLUS variants):	Update to V4.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/78647504/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200MP IM 155-5 PN ST (6ES7155-5AA00-0AB0): All versions < V4.1.0 affected by CVE-2019-13946	Update to V4.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/78647504/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200MP IM 155-5 PN ST (6AG1155-5AA00-7AB0): All versions < V4.1.0 affected by CVE-2019-13946	Update to V4.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/78647504/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200MP IM 155-5 PN ST TX RAIL (6AG2155-5AA00-4AB0): All versions < V4.1.0 affected by CVE-2019-13946	Update to V4.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/78647504/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200pro IM 154-3 PN HF (6ES7154-3AB00-0AB0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200pro IM 154-4 PN HF (6ES7154-4AB10-0AB0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN BA (6ES7155-6AR00-0AN0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN HF (incl. SIPLUS variants):	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/85624387/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN HF (6ES7155-6AU00-0CN0): All versions < V4.2.0 affected by CVE-2019-13946	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/85624387/ See further recommendations from section Workarounds and Mitigations

SIPLUS ET 200SP IM 155-6 PN HF (6AG1155-6AU00-4CN0): All versions < V4.2.0 affected by CVE-2019-13946	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/85624387/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP IM 155-6 PN HF (6AG1155-6AU00-2CN0): All versions < V4.2.0 affected by CVE-2019-13946	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/85624387/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP IM 155-6 PN HF T1 RAIL (6AG2155-6AU00-1CN0): All versions < V4.2.0 affected by CVE-2019-13946	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/85624387/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN ST (incl. SIPLUS variants):	Update to V4.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/78648144/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN ST (-Ax00) (incl. SIPLUS variants):	Update to V4.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/78648144/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN ST (6ES7155-6AU00-0BN0): All versions < V4.1.0 affected by CVE-2019-13946	Update to V4.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/78648144/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN ST BA (6ES7155-6AA00-0BN0): All versions < V4.1.0 affected by CVE-2019-13946	Update to V4.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/78648144/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP IM 155-6 PN ST (6AG1155-6AU00-7BN0): All versions < V4.1.0 affected by CVE-2019-13946	Update to V4.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/78648144/ See further recommendations from section Workarounds and Mitigations

SIPLUS ET 200SP IM 155-6 PN ST BA (6AG1155-6AA00-7BN0): All versions < V4.1.0 affected by CVE-2019-13946	Update to V4.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/78648144/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP IM 155-6 PN ST BA TX RAIL (6AG2155-6AA00-4BN0): All versions < V4.1.0 affected by CVE-2019-13946	Update to V4.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/78648144/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP IM 155-6 PN ST TX RAIL (6AG2155-6AU00-4BN0): All versions < V4.1.0 affected by CVE-2019-13946	Update to V4.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/78648144/ See further recommendations from section Workarounds and Mitigations
SIMATIC IPC Support, Package for VxWorks: All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC MV400 family:	Update to V7.0.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109793481/ See further recommendations from section Workarounds and Mitigations
SIMATIC MV420 SR-B (6GF3420-0AA20): All versions < V7.0.6 affected by CVE-2019-13946	Update to V7.0.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109793481/ See further recommendations from section Workarounds and Mitigations
SIMATIC MV420 SR-B Body (6GF3420-0AX20): All versions < V7.0.6 affected by CVE-2019-13946	Update to V7.0.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109793481/ See further recommendations from section Workarounds and Mitigations
SIMATIC MV420 SR-P (6GF3420-0AA40): All versions < V7.0.6 affected by CVE-2019-13946	Update to V7.0.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109793481/ See further recommendations from section Workarounds and Mitigations
SIMATIC MV420 SR-P Body (6GF3420-0AX40): All versions < V7.0.6 affected by CVE-2019-13946	Update to V7.0.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109793481/ See further recommendations from section Workarounds and Mitigations

SIMATIC MV440 HR (6GF3440-1GE10): All versions < V7.0.6 affected by CVE-2019-13946	Update to V7.0.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109793481/ See further recommendations from section Workarounds and Mitigations
SIMATIC MV440 SR (6GF3440-1CD10): All versions < V7.0.6 affected by CVE-2019-13946	Update to V7.0.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109793481/ See further recommendations from section Workarounds and Mitigations
SIMATIC MV440 UR (6GF3440-1LE10): All versions < V7.0.6 affected by CVE-2019-13946	Update to V7.0.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109793481/ See further recommendations from section Workarounds and Mitigations
SIMATIC PN/PN Coupler (incl. SIPLUS NET variants): All Versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC RF180C (6GT2002-0JD00): All versions affected by CVE-2019-13946	Currently no fix is planned Migrate to a successor product within the SIMATIC RF18xC/CI family, V1.3 (https://support.industry.siemens.com/cs/ww/en/view/109781665) or later version; for details refer to the phase-out announcement (https://support.industry.siemens.com/cs/ww/en/view/109783832) See further recommendations from section Workarounds and Mitigations
SIMATIC RF182C (6GT2002-0JD10): All versions affected by CVE-2019-13946	Currently no fix is planned Migrate to a successor product within the SIMATIC RF18xC/CI family, V1.3 (https://support.industry.siemens.com/cs/ww/en/view/109781665) or later version; for details refer to the phase-out announcement (https://support.industry.siemens.com/cs/ww/en/view/109783832) See further recommendations from section Workarounds and Mitigations
SIMATIC RF600R family: All versions < V3 affected by CVE-2019-13946	Update to V3.2.1 https://support.industry.siemens.com/cs/ww/en/view/109768501 See further recommendations from section Workarounds and Mitigations

SIMOTION C: All versions < V4.5 affected by CVE-2019-13946	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/31263919 See further recommendations from section Workarounds and Mitigations
SIMOTION D: All versions < V4.5 affected by CVE-2019-13946	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/31045047 See further recommendations from section Workarounds and Mitigations
SIMOTION P: All versions < V4.5 affected by CVE-2019-13946	Update to V4.5 or later version Please contact your Siemens representative for information on how to obtain the update. See further recommendations from section Workarounds and Mitigations
SINAMICS DCP: All Versions < V1.3 affected by CVE-2019-13946	Update to V1.3 https://support.industry.siemens.com/cs/ww/en/view/109773826/ See further recommendations from section Workarounds and Mitigations
SIPLUS NET CP 343-1 (6AG1343-1EX30-7XE0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS NET CP 343-1 Advanced (6AG1343-1GX31-4XE0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS NET CP 343-1 Lean (6AG1343-1CX10-2XE0): All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS NET CP 443-1 (6AG1443-1EX30-4XE0): All versions < V3.3 affected by CVE-2019-13946	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109817938/ See further recommendations from section Workarounds and Mitigations
SIPLUS NET CP 443-1 Advanced (6AG1443-1GX30-4XE0): All versions < V3.3 affected by CVE-2019-13946	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109817938/ See further recommendations from section Workarounds and Mitigations
SOFTNET-IE PNIO: All versions affected by CVE-2019-13946	Currently no fix is planned See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Disable PROFINET in products, where PROFINET is optional and not used in your environment
- Block incoming DCE-RPC packets (port 34964/udp) from untrusted networks

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 1616 and CP 1604 are PCI/PCI-104 cards for high-performance connection of field devices to Industrial Ethernet with PROFINET.

Development/Evaluation Kits for PROFINET IO are used to develop compact or modular PROFINET field devices.

PN/PN coupler is used for connecting two PROFINET networks.

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.

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

SCALANCE W products are wireless communication devices used to connect industrial components, like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs), according to the IEEE 802.11 standard (802.11ac, 802.11a/b/g/h, and/or 802.11n).

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

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 ET 200 Interface modules for PROFINET IO are used to connect field devices (IO Devices) to controllers (IO Controller) via PROFINET.

With the SIMATIC IPC Support Package for VxWorks, Siemens offers support for industrial computers (SIMATIC IPCs) for the VxWorks real-time operating system.

SIMATIC MV400 devices are stationary optical readers, used to reliably capture printed, lasered, drilled, punched and dotpeen codes on a variety of different surfaces.

PROFINET Driver is a development kit used to develop PROFINET IO controllers.

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).

SIMATIC RF182C is an RFID communication module for direct connection of SIMATIC identification systems to Ethernet/IP. SIMATIC RF182C is superseded by the SIMATIC RF18xC devices (RF185C, RF186C, RF188C).

SIMATIC RF185C, RF186C/CI, and RF188C/CI are communication modules for direct connection of SIMATIC identification systems to PROFINET IO/Ethernet and OPC UA.

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

With the SINAMICS converter series you can solve drive tasks in the low, medium and DC voltage range.

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

The SOFTNET product family includes several software applications for connecting programming devices to Industrial Ethernet and PROFIBUS.

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-2019-13946

Profinet-IO (PNIO) stack versions prior V06.00 do not properly limit internal resource allocation when multiple legitimate diagnostic package requests are sent to the DCE-RPC interface. This could lead to a denial of service condition due to lack of memory for devices that include a vulnerable version of the stack.

The security vulnerability could be exploited by an attacker with network access to an affected device. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise the availability of the device.

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/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Cybersecurity and Infrastructure Security Agency (CISA) for coordination efforts
- Yuval Ardon and Matan Dobrushin from OTORIO for coordinated disclosure

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 (2020-02-11):	Publication Date
V1.1 (2020-03-10):	Added affected product SOFTNET-IE PNIO
V1.2 (2020-03-12):	Additional information in section "Workarounds and Mitigations"
V1.3 (2020-08-11):	No changes - this version was never released
V1.4 (2020-08-11):	Added SIMATIC ET200ecoPN product variants (MLFB IDs) that are not affected
V1.5 (2020-09-08):	Informed about successor products for SIMATIC RF180C and RF182C
V1.6 (2020-12-08):	Added SIMOTION products; Updated information regarding successor products for SIMATIC RF180C and RF182C

V1.7 (2021-03-09):	Added ecoPN model (6ES7148-6JG00-0BB0) as not affected. Added update information for MV400
V1.8 (2021-09-14):	Added solution for SCALANCE X-200 switch family, explicitly list SCALANCE XB-200, XC-200, XP-200, XF-200BA and XR-300WG, as well as SCALANCE M-800 / S615 as separate products
V1.9 (2021-10-12):	Clarified affected ET200ecoPN models
V2.0 (2022-02-08):	No remediation planned for SIMATIC CP 343-1 (incl. Advanced, ERPC, Lean and related SIPLUS variants), SIMATIC CP 443-1 OPC UA, SIMATIC ET200 devices, and SOFTNET-IE PNIO
V2.1 (2022-04-12):	Added solution for SCALANCE X-300 switch family (incl. X408 and SIPLUS NET variants)
V2.2 (2022-06-14):	No fix planned for SIMATIC CP 443-1 Advanced and SIPLUS NET CP 443-1 Advanced
V2.3 (2023-04-11):	Added fix for SIMATIC CP 443-1 family
V2.4 (2024-07-09):	Listed affected products individually instead of product families (e.g., for SIMATIC MV400, SIMATIC ET 200AL/MP/SP/pro IM families); added affected SIPLUS devices (e.g., SIPLUS ET 200xx IM); corrected fix version for SIMATIC ET 200SP IM 155-6 PN HF

TERMS OF USE