# SSA-599968: Denial-of-Service Vulnerability in Profinet Devices

Publication Date: 2021-07-13
Last Update: 2024-06-11
Current Version: V1.6
CVSS v3.1 Base Score: 7.5

## SUMMARY

A vulnerability in affected devices could allow an attacker to perform a denial-of-service attack if a large amount of Profinet Discovery and Configuration Protocol (DCP) reset packets is sent to the affected devices.

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 specific countermeasures for products where fixes are not, or not yet available.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller:<br>All versions<br>affected by CVE-2020-28400 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200:<br>All versions<br>affected by CVE-2020-28400 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P:<br>All versions < V4.7<br>affected by CVE-2020-28400 | Update to V4.7 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109784253/<br>See further recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RM1224 family (6GK6108-4AM00):<br>All Versions < V6.4<br>affected by CVE-2020-28400 | Update to V6.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109794349/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M804PB (6GK5804-0AP00-2AA2):<br>All Versions < V6.4<br>affected by CVE-2020-28400 | Update to V6.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109794349/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M812-1 ADSL-Router (Annex A) (6GK5812-1AA00-2AA2):<br>All Versions < V6.4<br>affected by CVE-2020-28400 | Update to V6.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109794349/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE M812-1 ADSL-Router (Annex B) (6GK5812-1BA00-2AA2):<br>All Versions < V6.4<br>affected by CVE-2020-28400 | Update to V6.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109794349/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M816-1 ADSL-Router (Annex A) (6GK5816-1AA00-2AA2):<br>All Versions < V6.4<br>affected by CVE-2020-28400 | Update to V6.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109794349/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M816-1 ADSL-Router (Annex B) (6GK5816-1BA00-2AA2):<br>All Versions < V6.4<br>affected by CVE-2020-28400 | Update to V6.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109794349/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2):<br>All Versions < V6.4<br>affected by CVE-2020-28400 | Update to V6.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109794349/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M874-2 (6GK5874-2AA00-2AA2):<br>All Versions < V6.4<br>affected by CVE-2020-28400 | Update to V6.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109794349/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M874-3 (6GK5874-3AA00-2AA2):<br>All Versions < V6.4<br>affected by CVE-2020-28400 | Update to V6.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109794349/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M876-3 (EVDO) (6GK5876-3AA02-2BA2):<br>All Versions < V6.4<br>affected by CVE-2020-28400 | Update to V6.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109794349/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2):<br>All Versions < V6.4<br>affected by CVE-2020-28400 | Update to V6.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109794349/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2):<br>All Versions < V6.4<br>affected by CVE-2020-28400 | Update to V6.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109794349/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2):<br>All Versions < V6.4<br>affected by CVE-2020-28400 | Update to V6.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109794349/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE S615 (6GK5615-0AA00-2AA2):<br>All Versions < V6.4<br>affected by CVE-2020-28400 | Update to V6.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109794349/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE W1748-1 M12 (6GK5748-1GY01-0AA0):<br>All versions < V3.0.0<br>affected by CVE-2020-28400 | Update to V3.0.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808629/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE W1748-1 M12 (6GK5748-1GY01-0TA0):<br>All versions < V3.0.0<br>affected by CVE-2020-28400 | Update to V3.0.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808629/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE W1788-1 M12 (6GK5788-1GY01-0AA0):<br>All versions < V3.0.0<br>affected by CVE-2020-28400 | Update to V3.0.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808629/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE W1788-2 EEC M12 (6GK5788-2GY01-0TA0):<br>All versions < V3.0.0<br>affected by CVE-2020-28400 | Update to V3.0.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808629/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE W1788-2 M12 (6GK5788-2GY01-0AA0):<br>All versions < V3.0.0<br>affected by CVE-2020-28400 | Update to V3.0.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808629/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE W1788-2IA M12 (6GK5788-2HY01-0AA0):<br>All versions < V3.0.0<br>affected by CVE-2020-28400 | Update to V3.0.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808629/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE W-700 IEEE 802.11n family:<br>All versions<br>affected by CVE-2020-28400 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SCALANCE X200-4P IRT (6GK5200-4AH00-2BA3):<br>All Versions < V5.5.0<br>affected by CVE-2020-28400 | Update to V5.5.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109793952/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X201-3P IRT (6GK5201-3BH00-2BA3):<br>All Versions < V5.5.0<br>affected by CVE-2020-28400 | Update to V5.5.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109793952/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X201-3P IRT PRO (6GK5201-3JR00-2BA6):<br>All Versions < V5.5.0<br>affected by CVE-2020-28400 | Update to V5.5.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109793952/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X202-2IRT (6GK5202-2BB00-2BA3):<br>All Versions < V5.5.0<br>affected by CVE-2020-28400 | Update to V5.5.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109793952/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X202-2P IRT (6GK5202-2BH00-2BA3):<br>All Versions < V5.5.0<br>affected by CVE-2020-28400 | Update to V5.5.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109793952/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X202-2P IRT PRO (6GK5202-2JR00-2BA6):<br>All Versions < V5.5.0<br>affected by CVE-2020-28400 | Update to V5.5.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109793952/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X204-2 (6GK5204-2BB10-2AA3):<br>All versions < V5.2.5<br>affected by CVE-2020-28400 | Update to V5.2.5 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109801131/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE X204-2FM (6GK5204-2BB11-2AA3):<br>All versions < V5.2.5<br>affected by CVE-2020-28400 | Update to V5.2.5 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109801131/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X204-2LD (6GK5204-2BC10-2AA3):<br>All versions < V5.2.5<br>affected by CVE-2020-28400 | Update to V5.2.5 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109801131/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X204-2LD TS (6GK5204-2BC10-2CA2):<br>All versions < V5.2.5<br>affected by CVE-2020-28400 | Update to V5.2.5 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109801131/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X204-2TS (6GK5204-2BB10-2CA2):<br>All versions < V5.2.5<br>affected by CVE-2020-28400 | Update to V5.2.5 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109801131/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X204IRT (6GK5204-0BA00-2BA3):<br>All Versions < V5.5.0<br>affected by CVE-2020-28400 | Update to V5.5.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109793952/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X204IRT PRO (6GK5204-0JA00-2BA6):<br>All Versions < V5.5.0<br>affected by CVE-2020-28400 | Update to V5.5.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109793952/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X206-1 (6GK5206-1BB10-2AA3):<br>All versions < V5.2.5<br>affected by CVE-2020-28400 | Update to V5.2.5 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109801131/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X206-1LD (incl. SIPLUS NET variant):<br>All versions < V5.2.5<br>affected by CVE-2020-28400 | Update to V5.2.5 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109801131/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE X208 (incl. SIPLUS NET variant):<br>All versions < V5.2.5<br>affected by CVE-2020-28400 | Update to V5.2.5 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109801131/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X208PRO (6GK5208-0HA10-2AA6):<br>All versions < V5.2.5<br>affected by CVE-2020-28400 | Update to V5.2.5 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109801131/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X212-2 (6GK5212-2BB00-2AA3):<br>All versions < V5.2.5<br>affected by CVE-2020-28400 | Update to V5.2.5 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109801131/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X212-2LD (6GK5212-2BC00-2AA3):<br>All versions < V5.2.5<br>affected by CVE-2020-28400 | Update to V5.2.5 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109801131/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X216 (6GK5216-0BA00-2AA3):<br>All versions < V5.2.5<br>affected by CVE-2020-28400 | Update to V5.2.5 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109801131/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X224 (6GK5224-0BA00-2AA3):<br>All versions < V5.2.5<br>affected by CVE-2020-28400 | Update to V5.2.5 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109801131/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X302-7 EEC (2x 24V) (6GK5302-7GD00-2EA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X302-7 EEC (2x 24V, coated) (6GK5302-7GD00-2GA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE X302-7 EEC (2x 230V) (6GK5302-7GD00-4EA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X302-7 EEC (2x 230V, coated) (6GK5302-7GD00-4GA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X302-7 EEC (24V) (6GK5302-7GD00-1EA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X302-7 EEC (24V, coated) (6GK5302-7GD00-1GA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X302-7 EEC (230V) (6GK5302-7GD00-3EA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X302-7 EEC (230V, coated) (6GK5302-7GD00-3GA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X304-2FE (6GK5304-2BD00-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X306-1LD FE (6GK5306-1BF00-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE X307-2 EEC (2x 24V) (6GK5307-2FD00-2EA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-2 EEC (2x 24V, coated) (6GK5307-2FD00-2GA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-2 EEC (2x 230V) (6GK5307-2FD00-4EA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-2 EEC (2x 230V, coated) (6GK5307-2FD00-4GA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-2 EEC (24V) (6GK5307-2FD00-1EA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-2 EEC (24V, coated) (6GK5307-2FD00-1GA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-2 EEC (230V) (6GK5307-2FD00-3EA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-2 EEC (230V, coated) (6GK5307-2FD00-3GA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE X307-3 (6GK5307-3BL00-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-3 (6GK5307-3BL10-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-3LD (6GK5307-3BM00-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X307-3LD (6GK5307-3BM10-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2 (6GK5308-2FL00-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2 (6GK5308-2FL10-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2LD (6GK5308-2FM00-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2LD (6GK5308-2FM10-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE X308-2LH (6GK5308-2FN00-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2LH (6GK5308-2FN10-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2LH+ (6GK5308-2FP00-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2LH+ (6GK5308-2FP10-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2M (6GK5308-2GG00-2AA2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2M (6GK5308-2GG10-2AA2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2M PoE (6GK5308-2QG00-2AA2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2M PoE (6GK5308-2QG10-2AA2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE X308-2M TS (6GK5308-2GG00-2CA2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X308-2M TS (6GK5308-2GG10-2CA2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X310 (6GK5310-0FA00-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X310 (6GK5310-0FA10-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X310FE (6GK5310-0BA00-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X310FE (6GK5310-0BA10-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X320-1 FE (6GK5320-1BD00-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE X320-1-2LD FE (6GK5320-3BF00-2AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE X408-2 (6GK5408-2FD00-2AA2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XB-200:<br>All versions < V4.3<br>affected by CVE-2020-28400 | Update to V4.3 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109799569/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XC-200:<br>All versions < V4.3<br>affected by CVE-2020-28400 | Update to V4.3 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109799569/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XF201-3P IRT (6GK5201-3BH00-2BD2):<br>All Versions < V5.5.0<br>affected by CVE-2020-28400 | Update to V5.5.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109793952/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XF202-2P IRT (6GK5202-2BH00-2BD2):<br>All Versions < V5.5.0<br>affected by CVE-2020-28400 | Update to V5.5.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109793952/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XF204 (6GK5204-0BA00-2AF2):<br>All versions < V5.2.5<br>affected by CVE-2020-28400 | Update to V5.2.5 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109801131/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XF204-2 (incl. SIPLUS NET variant):<br>All versions < V5.2.5<br>affected by CVE-2020-28400 | Update to V5.2.5 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109801131/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XF204-2BA IRT (6GK5204-2AA00-2BD2):<br>All Versions < V5.5.0<br>affected by CVE-2020-28400 | Update to V5.5.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109793952/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XF204IRT (6GK5204-0BA00-2BF2):<br>All Versions < V5.5.0<br>affected by CVE-2020-28400 | Update to V5.5.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109793952/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XF206-1 (6GK5206-1BC00-2AF2):<br>All versions < V5.2.5<br>affected by CVE-2020-28400 | Update to V5.2.5 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109801131/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XF208 (6GK5208-0BA00-2AF2):<br>All versions < V5.2.5<br>affected by CVE-2020-28400 | Update to V5.2.5 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109801131/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XF-200BA:<br>All versions < V4.3<br>affected by CVE-2020-28400 | Update to V4.3 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109799569/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XM-400 Family:<br>All versions < V6.3.1<br>affected by CVE-2020-28400 | Update to V6.3.1 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109782067/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XP-200:<br>All versions < V4.3<br>affected by CVE-2020-28400 | Update to V4.3 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109799569/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (2x 24V, ports on front) (6GK5324-4GG00-2ER2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (2x 24V, ports on front) (6GK5324-4GG10-2ER2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XR324-4M EEC (2x 24V, ports on rear) (6GK5324-4GG00-2JR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (2x 24V, ports on rear) (6GK5324-4GG10-2JR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front) (6GK5324-4GG00-4ER2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front) (6GK5324-4GG10-4ER2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG00-4JR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG10-4JR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (24V, ports on front) (6GK5324-4GG00-1ER2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (24V, ports on front) (6GK5324-4GG10-1ER2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XR324-4M EEC (24V, ports on rear) (6GK5324-4GG00-1JR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (24V, ports on rear) (6GK5324-4GG10-1JR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front) (6GK5324-4GG00-3ER2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front) (6GK5324-4GG10-3ER2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG00-3JR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG10-3JR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M PoE (24V, ports on front) (6GK5324-4QG00-1AR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M PoE (24V, ports on rear) (6GK5324-4QG00-1HR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XR324-4M PoE (230V, ports on front) (6GK5324-4QG00-3AR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M PoE (230V, ports on rear) (6GK5324-4QG00-3HR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-4M PoE TS (24V, ports on front) (6GK5324-4QG00-1CR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-12M (24V, ports on front) (6GK5324-0GG00-1AR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-12M (24V, ports on front) (6GK5324-0GG10-1AR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-12M (24V, ports on rear) (6GK5324-0GG00-1HR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-12M (24V, ports on rear) (6GK5324-0GG10-1HR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-12M (230V, ports on front) (6GK5324-0GG00-3AR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE XR324-12M (230V, ports on front) (6GK5324-0GG10-3AR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-12M (230V, ports on rear) (6GK5324-0GG00-3HR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-12M (230V, ports on rear) (6GK5324-0GG10-3HR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-12M TS (24V) (6GK5324-0GG00-1CR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR324-12M TS (24V) (6GK5324-0GG10-1CR2):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE XR500:<br>All versions < V6.3.1<br>affected by CVE-2020-28400 | Update to V6.3.1 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109782065/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC CFU DIQ (6ES7655-5PX31-1XX0):<br>All versions < V2.0.0<br>affected by CVE-2020-28400 | Update to V2.0.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109781049/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC CFU PA (6ES7655-5PX11-0XX0):<br>All versions < V2.0.0<br>affected by CVE-2020-28400 | Update to V2.0.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109754628/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC CM 1542-1:<br>All versions < V3.0<br>affected by CVE-2020-28400 | Update to V3.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109801629/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC CP1616/CP1604:<br>All Versions >= V2.7<br>affected by CVE-2020-28400 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC CP 1626 (6GK1162-6AA01):<br>All versions<br>affected by CVE-2020-28400 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC IE/PB-LINK:<br>All versions >= V3<br>affected by CVE-2020-28400 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC MV540 H (6GF3540-0GE10):<br>All versions < V3.0<br>affected by CVE-2020-28400 | Update to V3.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109795469/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC MV540 S (6GF3540-0CD10):<br>All versions < V3.0<br>affected by CVE-2020-28400 | Update to V3.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109795469/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC MV550 H (6GF3550-0GE10):<br>All versions < V3.0<br>affected by CVE-2020-28400 | Update to V3.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109795469/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC MV550 S (6GF3550-0CD10):<br>All versions < V3.0<br>affected by CVE-2020-28400 | Update to V3.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109795469/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC MV560 U (6GF3560-0LE10):<br>All versions < V3.0<br>affected by CVE-2020-28400 | Update to V3.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109795469/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC MV560 X (6GF3560-0HE10):<br>All versions < V3.0<br>affected by CVE-2020-28400 | Update to V3.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109795469/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC NET DK-16xx PN IO:<br>All Versions >= V2.7<br>affected by CVE-2020-28400 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC Power Line Booster PLB, Base Module (6ES7972-5AA10-0AB0):<br>All versions<br>affected by CVE-2020-28400 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC PROFINET Driver:<br>All versions < V2.3<br>affected by CVE-2020-28400 | Update to V2.3 or later version<br>https://support.industry.siemens.com/cs/de/en/view/109802422/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1200 CPU family (incl. SIPLUS variants):<br>All Versions < V4.5<br>affected by CVE-2020-28400 | Update to V4.5 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109793280/<br>See further recommendations from section Workarounds and Mitigations |
| SIMOCODE pro V Ethernet/IP (incl. SIPLUS variants):<br>All versions < V1.1.3<br>affected by CVE-2020-28400 | Update to V1.1.3 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109756912/<br>See further recommendations from section Workarounds and Mitigations |
| SIMOCODE pro V PROFINET (incl. SIPLUS variants):<br>All versions < V2.1.3<br>affected by CVE-2020-28400 | Update to V2.1.3 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109749989/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS NET SCALANCE X308-2 (6AG1308-2FL10-4AA3):<br>All versions < V4.1.4<br>affected by CVE-2020-28400 | Update to V4.1.4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109808359/<br>See further recommendations from section Workarounds and Mitigations |
| SOFTNET-IE PNIO:<br>All versions<br>affected by CVE-2020-28400 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |

## WORKAROUNDS AND MITIGATIONS

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

- Block incoming Profinet Discovery and Configuration Protocol (DCP) packets (Ethertype 0x8892, Frame-ID: 0xfefe) from untrusted networks
- Disable Profinet in products, where Profinet is optional and not used in your environment

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.

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

SIMATIC CP 1626 are PCI express cards for connecting field devices to Industrial Ethernet with PROFINET.

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

IE/PB-Link devices enable existing PROFIBUS devices to be integrated into a PROFINET application.

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

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

SCALANCE 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 W-1700 products are wireless communication devices based on IEEE 802.11ac standard. They are used to connect all to sorts of WLAN devices (Access Points or Clients, depending on the operating mode) with a strong focus on industrial components, like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs) and others.

SCALANCE W-700 products are wireless communication devices based on IEEE 802.11ax or 802.11n standard. They are used to connect all to sorts of WLAN devices (Access Points or Clients, depending on the operating mode) with a strong focus on industrial components, like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs) and others.

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

SIMATIC Compact Field Unit (SIMATIC CFU) is a smart field distributor for use as an I/O device on PROFINET of an automation system.

The SIMATIC CM 1542-1 communication module is used to connect S7-1500 controllers to PROFINET as IO-Controller.

The Development Kit DK-16xx PN IO permits an easy integration of CP 1616 and CP 1604 in non-Windows operating system environments.

SIMATIC MV500 products 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.

The SIMATIC Power Line Booster system is a communication system for data transmission on conductive media.

SIMATIC S7-300, S7-400, S7-1200 CPU and S7-1500 CPU controllers have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIMOCODE pro is a modular motor management system that combines all required protection, monitoring, safety and control functions for motor feeders.

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

SINUMERIK CNC offers automation solutions for the shop floor, job shops and large serial production environments.

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 SIPLUS HCS 4x00 heating control system is used to control and switch heaters in industry control und operation e.g. quartz, ceramic, flash, halogen or infrared heaters.

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-2020-28400

Affected devices contain a vulnerability that allows an unauthenticated attacker to trigger a denial-of-service condition. The vulnerability can be triggered if a large amount of DCP reset packets are sent to 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-770: Allocation of Resources Without Limits or Throttling |

## ADDITIONAL INFORMATION

This vulnerability has been discovered internally by Siemens.

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 (2021-07-13): | Publication Date |
| V1.1 (2021-08-10): | Added solution for SCALANCE XR-300WG, SCALANCE XB-200, SCALANCE XP-200, SCALANCE XC-200, SCALANCE XF-200 and EK-ERTEC 200P |
| V1.2 (2021-09-14): | Added solution for SCALANCE X-200 switch family and SIMATIC NET CM 1542-1 |
| V1.3 (2021-10-12): | Added solution for SIMATIC PROFINET Driver |
| V1.4 (2022-02-08): | Clarified that no remediation is planned for SCALANCE W700 and SCALANCE W1700, SIMATIC CP 1604, SIMATIC CP 1616, and SIMATIC CP 1626 |
| V1.5 (2022-04-12): | Added solution for SCALANCE X-300 switch family (incl. X408 and SIPLUS NET variants) and SCALANCE W-1700 (11ac) family |
| V1.6 (2024-06-11): | Added fix for SIMATIC CFU PA/DIQ; fix planned for SIMATIC IE/PB-LINK |

## TERMS OF USE