Siemens Security Advisory by Siemens ProductCERT

SSA-599968: Denial of Service Vulnerability in Profinet Devices

Publication Date:	2021-07-13
Last Update:	2026-04-14
Current Version:	V1.9
CVSS v3.1 Base Score:	7.5
CVSS v4.0 Base Score:	8.7

▼ SUMMARY

A vulnerability in affected devices could allow an attacker to perform a denial ofservice 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 recommends specific countermeasures for products where fixes are not, or not yet available.

▼ KNOWN AFFECTED PRODUCTS

Un-/Collapse All

Affected Product and Versions	Remediation
Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller All versions affected by CVE-2020-28400	Currently no fix is planned See further recommendations from section Mitigations
Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200 All versions affected by CVE-2020-28400	Currently no fix is planned See further recommendations from section Mitigations
Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P All versions < V4.7 affected by CVE-2020-28400	Update to V4.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109784253/ See further recommendations from section Mitigations
SCALANCE M-800 family (incl. S615, MUM-800 and RM1224)	Show more details
SCALANCE W-700 IEEE 802.11n family	Show more details
SCALANCE W-1700 IEEE 802.11ac family	Show more details
SCALANCE X-200 family (incl. SIPLUS NET variants)	Show more details
SCALANCE X-200IRT family (incl. SIPLUS NET variants)	Show more details
SCALANCE X-300 family (incl. X408 and SIPLUS NET variants)	Show more details

SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG family	Show more details
SCALANCE XM-400/XR-500 family	Show more details
SIMATIC CFU DIQ (6ES7655-5PX31-1XX0) All versions < V2.0.0 affected by CVE-2020-28400	Update to V2.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109781049/ See further recommendations from section Mitigations
SIMATIC CFU PA (6ES7655-5PX11-0XX0) All versions < V2.0.0 affected by CVE-2020-28400	Update to V2.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109754628/ See further recommendations from section Mitigations
SIMATIC CM 1542-1 (6GK7542-1AX00-0XE0) All versions < V3.0 affected by CVE-2020-28400	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109801629/ See further recommendations from section Mitigations
SIMATIC CP 1604 (6GK1160-4AA01) All Versions >= V2.7 affected by CVE-2020-28400	Currently no fix is planned See further recommendations from section Mitigations
SIMATIC CP 1616 (6GK1161-6AA02) All Versions >= V2.7 affected by CVE-2020-28400	Currently no fix is planned See further recommendations from section Mitigations
SIMATIC CP 1626 (6GK1162-6AA01) All versions affected by CVE-2020-28400	Currently no fix is planned See further recommendations from section Mitigations
SIMATIC IE/PB-LINK All versions >= V3 affected by CVE-2020-28400	Currently no fix is planned See further recommendations from section Mitigations
SIMATIC MV500 family	Show more details
SIMATIC NET DK-16xx PN IO All Versions >= V2.7 affected by CVE-2020-28400	Currently no fix is planned See further recommendations from section Mitigations
SIMATIC Power Line Booster PLB, Base Module (6ES7972-5AA10-0AB0) All versions affected by CVE-2020-28400	Currently no fix is planned See further recommendations from section Mitigations
SIMATIC PROFINET Driver All versions < V2.3 affected by CVE-2020-28400	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109802423/ See further recommendations from section Mitigations
SIMATIC S7-1200 CPU V4 family (incl. SIPLUS variants)	Show more details
SIMOCODE pro V Ethernet/IP (incl. SIPLUS variants)	Show more details
SIMOCODE pro V PROFINET	Show more details

SOFTNET-IE PNIO All versions affected by CVE-2020-28400	Currently no fix is planned See further recommendations from section Mitigations

▼ MITIGATIONS

Siemens has identified the following specific 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 Profinet Discovery and Configuration Protocol (DCP) packets (Ethertype 0x8892, Frame-ID: 0xfefe) from untrusted networks

Product-specific remediations or mitigations can be found in the section Known Affected Products.
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

▼ VULNERABILITY DESCRIPTION

Un-/Collapse All

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 v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4.0 Base Score	8.7
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-770: Allocation of Resources Without Limits or Throttling

▼ 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	(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 fix 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
V1.7	(2024-11-12):	Added fix for SCALANCE XR-300WG family (was no longer listed since V1.5 of the SSA); consolidated and expanded list of affected SCALANCE product families, incl. MLFB information
V1.8	(2024-12-10):	Clarified that no fix is planned for SIMATIC IE/PB-LINK; Added CVSSv4.0 vector
V1.9	(2026-04-14):	Added fix for SCALANCE W-700 IEEE 802.11n family. Expanded list of affected SIMATIC S7-1200 CPU products, incl. MLFB information

▼ TERMS OF USE