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

Publication Date: 2021-07-13
Last Update: 2021-10-12
Current Version: V1.3
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 updates for several affected products and recommends to update to the latest versions. Siemens is preparing further updates and recommends specific countermeasures for products where updates 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: All versions	See recommendations from section Workarounds and Mitigations
Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200: All versions	See recommendations from section Workarounds and Mitigations
Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P: All versions < V4.7	Update to V4.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109784253/
RUGGEDCOM RM1224: All Versions < V6.4	Update to V6.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109794349/
SCALANCE M-800: All Versions < V6.4	Update to V6.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109794349/
SCALANCE S615: All Versions < V6.4	Update to V6.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109794349/
SCALANCE W700 IEEE 802.11n: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE W1700 IEEE 802.11ac: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X200-4 P IRT: All Versions < V5.5.0	Update to V5.5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109793952/

SCALANCE X201-3P IRT: All Versions < V5.5.0	Update to V5.5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109793952/
SCALANCE X201-3P IRT PRO: All Versions < V5.5.0	Update to V5.5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109793952/
SCALANCE X202-2 IRT: All Versions < V5.5.0	Update to V5.5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109793952/
SCALANCE X202-2P IRT (incl. SIPLUS NET variant): All Versions < V5.5.0	Update to V5.5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109793952/
SCALANCE X202-2P IRT PRO: All Versions < V5.5.0	Update to V5.5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109793952/
SCALANCE X204 IRT: All Versions < V5.5.0	Update to V5.5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109793952/
SCALANCE X204 IRT PRO: All Versions < V5.5.0	Update to V5.5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109793952/
SCALANCE X204-2 (incl. SIPLUS NET variant): All versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X204-2FM: All versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X204-2LD (incl. SIPLUS NET variant): All versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X204-2LD TS: All versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X204-2TS: All versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X206-1: All versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X206-1LD (incl. SIPLUS NET variant): All versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X208 (incl. SIPLUS NET variant): All versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/

SCALANCE X208PRO: All versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X212-2: All versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X212-2LD: All versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X216: All versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X224: All versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE X302-7EEC: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X304-2FE: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X306-1LDFE: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X307-2EEC: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X307-3: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X307-3LD: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X308-2 (incl. SIPLUS NET variant): All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X308-2LD: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH+: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X308-2M: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X308-2M PoE: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X308-2M TS: All versions	See recommendations from section Workarounds and Mitigations

SCALANCE X310: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X310FE: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X320-1FE: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X320-3LDFE: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XB-200: All versions < V4.3	Update to V4.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109799569/
SCALANCE XC-200: All versions < V4.3	Update to V4.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109799569/
SCALANCE XF201-3P IRT: All Versions < V5.5.0	Update to V5.5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109793952/
SCALANCE XF202-2P IRT: All Versions < V5.5.0	Update to V5.5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109793952/
SCALANCE XF204: All versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE XF204 IRT: All Versions < V5.5.0	Update to V5.5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109793952/
SCALANCE XF204-2 (incl. SIPLUS NET variant): All versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE XF204-2BA IRT: All Versions < V5.5.0	Update to V5.5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109793952/
SCALANCE XF206-1: All versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE XF208: All versions < V5.2.5	Update to V5.2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109801131/
SCALANCE XF-200BA: All versions < V4.3	Update to V4.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109799569/
SCALANCE XM400: All versions < V6.3.1	Update to V6.3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109782067/

SCALANCE XP-200: All versions < V4.3	Update to V4.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109799569/
SCALANCE XR324-4M EEC: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE TS: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M TS: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XR500: All versions < V6.3.1	Update to V6.3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109782065/
SCALANCE XR-300WG: All versions < V4.3	Update to V4.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109799569/
SIMATIC CFU PA: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC CM 1542-1: All versions < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109801629/
SIMATIC CP1616/CP1604: All Versions >= V2.7	See recommendations from section Workarounds and Mitigations
SIMATIC CP1626: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IE/PB-LINK V3: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC MV500 family: All versions < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109795469/
SIMATIC NET DK-16xx PN IO: All Versions >= V2.7	See recommendations from section Workarounds and Mitigations
SIMATIC Power Line Booster PLB, Base Module (MLFB: 6ES7972-5AA10-0AB0): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC PROFINET Driver: All versions < V2.3	Update to V2.3 or later version https://support.industry.siemens.com/cs/de/en/view/109802422/

SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All Versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109793280/
SIMOCODE proV Ethernet/IP: All versions < V1.1.3	Update to V1.1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109756912/
SIMOCODE proV PROFINET: All versions < V2.1.3	Update to V2.1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109749989/
SOFTNET-IE PNIO: All versions	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

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

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.

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

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).

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

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

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

SIMOCODE is the flexible and modular motor management system for low-voltage motors.

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

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

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

The SINAMICS converter family is used to control a wide variety of drives, especially in mechanical engineering and plant construction.

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.

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

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-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

TERMS OF USE