SSA-446448: Denial of Service Vulnerability in PROFINET Stack Integrated on Interniche Stack

Publication Date: 2022-04-12
Last Update: 2022-08-09
Current Version: V1.3
CVSS v3.1 Base Score: 5.3

SUMMARY

The PROFINET (PNIO) stack, when integrated with the Interniche IP stack, contains a vulnerability that could allow an attacker to cause a denial of service condition on affected industrial products.

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
SIMATIC CFU DIQ (6ES7655-5PX31-1XX0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC CFU PA (6ES7655-5PX11-0XX0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC ET200AL IM157-1 PN: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, CM 8x IO-Link, M12-L (6ES7148-6JG00-0BB0): All versions >= V5.1.1	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, DI 8x24VDC, M12-L (6ES7141-6BG00-0BB0): All versions >= V5.1.1	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, DI 16x24VDC, M12-L (6ES7141-6BH00-0BB0): All versions >= V5.1.1	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, DIQ 16x24VDC/2A, M12-L (6ES7143-6BH00-0BB0): All versions >= V5.1.1	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, DQ 8x24VDC/0,5A, M12-L (6ES7142-6BG00-0BB0): All versions >= V5.1.1	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, DQ 8x24VDC/2A, M12-L (6ES7142-6BR00-0BB0): All versions >= V5.1.1	Currently no fix is planned See recommendations from section Workarounds and Mitigations

 © Siemens 2022

SIMATIC ET200MP IM155-5 PN HF (incl. SIPLUS variants): All versions >= V4.2	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 MF HF: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 PN HA (incl. SIPLUS variants): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 PN HF (incl. SIPLUS variants): All versions >= V4.2	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 PN/2 HF (incl. SIPLUS variants): All versions >= V4.2	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 PN/3 HF (incl. SIPLUS variants): All versions >= V4.2	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC PN/MF Coupler (6ES7158-3MU10-0XA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC PN/PN Coupler (6ES7158-3AD10-0XA0): All versions >= 4.2	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 H V6 CPU family (incl. SIPLUS variants): All versions < V6.0.10	Update to V6.0.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109474550/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants): All versions < V8.2.3	Update to V8.2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109476571 See further recommendations from section Workarounds and Mitigations
SIMATIC S7-410 V10 CPU family (incl. SIPLUS variants): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V2.0.0	Update to V2.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC TDC CP51M1: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC TDC CPU555: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC WinAC RTX: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMIT Simulation Platform: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SINAMICS DCM: All versions with Ethernet interface	Currently no fix is available See recommendations from section Workarounds and Mitigations
SINAMICS G110M: All versions with Ethernet interface	Currently no fix is available See recommendations from section Workarounds and Mitigations
SINAMICS G115D: All versions with Ethernet interface	Currently no fix is available See recommendations from section Workarounds and Mitigations
SINAMICS G120 (incl. SIPLUS variants): All versions with Ethernet interface	Currently no fix is available See recommendations from section Workarounds and Mitigations
SINAMICS G130: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SINAMICS G150: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SINAMICS S110: All versions with Ethernet interface	Currently no fix is available See recommendations from section Workarounds and Mitigations
SINAMICS S120 (incl. SIPLUS variants): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SINAMICS S150: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SINAMICS S210: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

SINAMICS V90: All versions with Ethernet interface	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPLUS HCS4200 CIM4210 (6BK1942-1AA00-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS HCS4200 CIM4210C (6BK1942-1AA00-0AA1): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS HCS4300 CIM4310 (6BK1943-1AA00-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS NET PN/PN Coupler (6AG2158-3AD10-4XA0): All versions >= 4.2	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:

- Limit access to port 102/tcp to trusted users and systems only

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

PN/MF coupler is used to connect an EtherNet/IP network to a PROFINET subnet or to interconnect two PROFINET subnets.

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

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

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

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

Products of the Siemens SIMATIC S7-300 CPU family have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

Products in the SIMATIC S7-400 CPU family have been designed for process control in industrial environments. They are used worldwide, e.g. in the automotive industry, mechanical equipment manufacture, warehousing systems, building engineering, steel industry, power generation and distribution, pharmaceuticals, food and beverages industry, or chemical industry.

SIMATIC TDC is a multiprocessor automation system for drive, control and technology tasks. The system is used particularly for large plants.

SIMATIC WinAC RTX is a SIMATIC software controller for PC-based automation solutions.

SIMIT Simluation Platform allows the simulation of plant setups in order to anticipate faults in the early planning phase.

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

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.

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-2022-25622

The PROFINET (PNIO) stack, when integrated with the Interniche IP stack, improperly handles internal resources for TCP segments where the minimum TCP-Header length is less than defined.

This could allow an attacker to create a denial of service condition for TCP services on affected devices by sending specially crafted TCP segments.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2022-04-12):	Publication Date
V1.1 (2022-06-14):	Added ET200SP/MP/AL/EcoPN, PN/xx Coupler, SIPLUS HCS4x00 and SINAMICS products to the list of affected products
V1.2 (2022-07-12):	Added SINAMICS S110/V90/DCM products to the list of affected products. Additional details added to SINAMICS affected versions
V1.3 (2022-08-09):	Added fix for SIMATIC S7-410 CPU family

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.