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

Publication Date: 2022-04-12
Last Update: 2024-07-09
Current Version: V2.2
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 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.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC CFU DIQ (6ES7655-5PX31-1XX0): All versions < V2.0.0 affected by CVE-2022-25622	Update to V2.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109781049/ See further recommendations from section Workarounds and Mitigations
SIMATIC CFU PA (6ES7655-5PX11-0XX0): All versions < V2.0.0 affected by CVE-2022-25622	Update to V2.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109754628/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, AI 8xRTD/TC, M12-L (6ES7144-6JF00-0BB0): All versions >= V5.1.1 < V5.1.2 affected by CVE-2022-25622	Update to V5.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109955667/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, CM 4x IO-Link, M12-L (6ES7148-6JE00-0BB0): All versions >= V5.1.1 affected by CVE-2022-25622	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 affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, CM 8x IO-Link, M12-L (6ES7148-6JJ00-0BB0): All versions >= V5.1.1 affected by CVE-2022-25622	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 < V5.1.2 affected by CVE-2022-25622	Update to V5.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109798525/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, DI 16x24VDC, M12-L (6ES7141-6BH00-0BB0): All versions >= V5.1.1 < V5.1.2 affected by CVE-2022-25622	Update to V5.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109798527/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, DIQ 16x24VDC/2A, M12-L (6ES7143-6BH00-0BB0): All versions >= V5.1.1 < V5.1.3 affected by CVE-2022-25622	Update to V5.1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109798530/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, DQ 8x24VDC/0,5A, M12-L (6ES7142-6BG00-0BB0): All versions >= V5.1.1 < V5.1.2 affected by CVE-2022-25622	Update to V5.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109798528/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, DQ 8x24VDC/2A, M12-L (6ES7142-6BR00-0BB0): All versions >= V5.1.1 < V5.1.2 affected by CVE-2022-25622	Update to V5.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109798529/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200AL IM 157-1 PN (6ES7157-1AB00-0AB0): All versions affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200MP IM 155-5 PN HF (incl. SIPLUS variants):	Currently no fix is planned See 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-2022-25622	Currently no fix is planned See 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-2022-25622	Currently no fix is planned See 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-2022-25622	Currently no fix is planned See 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-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200pro IM 154-8 PN/DP CPU (6ES7154-8AB01-0AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/47354502/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200pro IM 154-8F PN/DP CPU (6ES7154-8FB01-0AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/47354578/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200pro IM 154-8FX PN/DP CPU (6ES7154-8FX00-0AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/62612377/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200S IM 151-8 PN/DP CPU (6ES7151-8AB01-0AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/47353723/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200S IM 151-8F PN/DP CPU (6ES7151-8FB01-0AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/47354354/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 MF HF (6ES7155-6MU00-0CN0): All versions affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN HA (incl. SIPLUS variants): All versions affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN HF (incl. SIPLUS variants):	Currently no fix is planned See 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-2022-25622	Currently no fix is planned See 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-2022-25622	Currently no fix is planned See 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-2022-25622	Currently no fix is planned See 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-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN/2 HF (incl. SIPLUS variants):	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN/2 HF (6ES7155-6AU01-0CN0): All versions >= V4.2.0 affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP IM 155-6 PN HF (6AG1155-6AU01-2CN0): All versions >= V4.2.0 affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP IM 155-6 PN HF (6AG1155-6AU01-7CN0): All versions >= V4.2.0 affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP IM 155-6 PN HF T1 RAIL (6AG2155-6AU01-1CN0): All versions >= V4.2.0 affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP IM 155-6 PN HF TX RAIL (6AG2155-6AU01-4CN0): All versions >= V4.2.0 affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN/3 HF (6ES7155-6AU30-0CN0): All versions >= V4.2.0 affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC PN/MF Coupler (6ES7158-3MU10-0XA0): All versions affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC PN/PN Coupler (6ES7158-3AD10-0XA0): All versions >= 4.2 affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC S7-300 CPU 314C-2 PN/DP (6ES7314-6EH04-0AB0): All versions < V3.3.19 affected by CVE-2022-25622	Update to V3.3.19 or later version https://support.industry.siemens.com/cs/ww/en/view/51466769/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 315-2 PN/DP (6ES7315-2EH14-0AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/40360647/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 315F-2 PN/DP (6ES7315-2FJ14-0AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/40944925/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 315T-3 PN/DP (6ES7315-7TJ10-0AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/85049260/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 317-2 PN/DP (6ES7317-2EK14-0AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/40362228/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 317F-2 PN/DP (6ES7317-2FK14-0AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/40945128/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 317T-3 PN/DP (6ES7317-7TK10-0AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/85059804/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 317TF-3 PN/DP (6ES7317-7UL10-0AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/85063017/ See further recommendations from section Workarounds and Mitigations

SIMATIC S7-300 CPU 319-3 PN/DP (6ES7318-3EL01-0AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/44442927/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 319F-3 PN/DP (6ES7318-3FL01-0AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/44443101/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 412-2 PN V7 (6ES7412-2EK07-0AB0): All versions affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 414-3 PN/DP V7 (6ES7414-3EM07-0AB0): All versions affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 414F-3 PN/DP V7 (6ES7414-3FM07-0AB0): All versions affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 416-3 PN/DP V7 (6ES7416-3ES07-0AB0): All versions affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 416F-3 PN/DP V7 (6ES7416-3FS07-0AB0): All versions affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 H V6 CPU family (incl. SIPLUS variants): All versions < V6.0.10 affected by CVE-2022-25622	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 S7-410 V8 CPU family (incl. SIPLUS variants): All versions < V8.2.3 affected by CVE-2022-25622	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 < V10.1.1 affected by CVE-2022-25622	Update to V10.1.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109773044/ See further recommendations from section Workarounds and Mitigations

SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V2.0.0 affected by CVE-2022-25622	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 < V1.1.10 affected by CVE-2022-25622	Update to V1.1.10 or later version https://support.industry.siemens.com/cs/ww/en/view/27049282/ See further recommendations from section Workarounds and Mitigations
SIMATIC TDC CPU555: All versions < V1.2.1 affected by CVE-2022-25622	Update to V1.2.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109740119/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinAC RTX 2010 (6ES7671-0RC08-0YA0): All versions affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC WinAC RTX F 2010 (6ES7671-1RC08-0YA0): All versions affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SINAMICS DCM: All versions < V1.5 SP1 with Ethernet interface affected by CVE-2022-25622	Update to V1.5 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/44029688/ See further recommendations from section Workarounds and Mitigations
SINAMICS G110M: All versions < V4.7.14 with Ethernet interface affected by CVE-2022-25622	Update to V4.7.14 or later version https://support.industry.siemens.com/cs/ww/en/view/109817231/ See further recommendations from section Workarounds and Mitigations
SINAMICS G115D: All versions < V4.7.14 with Ethernet interface affected by CVE-2022-25622	Update to V4.7.14 or later version https://support.industry.siemens.com/cs/ww/en/view/109817231/ See further recommendations from section Workarounds and Mitigations
SINAMICS G120 (incl. SIPLUS variants): All versions < V4.7 SP14 with Ethernet interface affected by CVE-2022-25622	Update to V4.7 SP14 or later version https://support.industry.siemens.com/cs/ww/en/view/109817231/ See further recommendations from section Workarounds and Mitigations

SINAMICS G130: All versions < V5.2.3.13 affected by CVE-2022-25622	Update to V5.2.3.13 or later version https://support.industry.siemens.com/cs/ww/en/view/109764679/ See further recommendations from section Workarounds and Mitigations
SINAMICS G150: All versions < V5.2.3.13 affected by CVE-2022-25622	Update to V5.2.3.13 or later version https://support.industry.siemens.com/cs/ww/en/view/109764679/ See further recommendations from section Workarounds and Mitigations
SINAMICS S110: All versions with Ethernet interface affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SINAMICS S120 (incl. SIPLUS variants): All versions < V5.2 SP3 HF13 affected by CVE-2022-25622	Update to V5.2 SP3 HF13 or later version https://support.industry.siemens.com/cs/ww/en/view/109780844/ See further recommendations from section Workarounds and Mitigations
SINAMICS S150: All versions < V5.2.3.13 affected by CVE-2022-25622	Update to V5.2.3.13 or later version https://support.industry.siemens.com/cs/ww/en/view/109764679/ See further recommendations from section Workarounds and Mitigations
SINAMICS S210 (6SL5...): All versions < V5.2 SP3 HF18 affected by CVE-2022-25622	Update to V5.2 SP3 HF18 or later version https://support.industry.siemens.com/cs/ww/en/view/109945645/ See further recommendations from section Workarounds and Mitigations
SINAMICS V90: All versions < V1.04.04 with Ethernet interface affected by CVE-2022-25622	Update to V1.04.04 or later version https://support.industry.siemens.com/cs/ww/en/view/109746210/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200S IM 151-8 PN/DP CPU (6AG1151-8AB01-7AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/47353723/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200S IM 151-8F PN/DP CPU (6AG1151-8FB01-2AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/47354354/ See further recommendations from section Workarounds and Mitigations

SIPLUS HCS4200 CIM4210 (6BK1942-1AA00-0AA0): All versions affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS HCS4200 CIM4210C (6BK1942-1AA00-0AA1): All versions affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS HCS4300 CIM4310 (6BK1943-1AA00-0AA0): All versions affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS NET PN/PN Coupler (6AG2158-3AD10-4XA0): All versions >= 4.2 affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 314C-2 PN/DP (6AG1314-6EH04-7AB0): All versions < V3.3.19 affected by CVE-2022-25622	Update to V3.3.19 or later version https://support.industry.siemens.com/cs/ww/en/view/51466769/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 315-2 PN/DP (6AG1315-2EH14-7AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/40360647/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 315F-2 PN/DP (6AG1315-2FJ14-2AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/40944925/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 317-2 PN/DP (6AG1317-2EK14-7AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/40362228/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 317F-2 PN/DP (6AG1317-2FK14-2AB0): All versions < V3.2.19 affected by CVE-2022-25622	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/40945128/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-400 CPU 414-3 PN/DP V7 (6AG1414-3EM07-7AB0): All versions affected by CVE-2022-25622	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIPLUS S7-400 CPU 416-3 PN/DP V7 (6AG1416-3ES07-7AB0): All versions affected by CVE-2022-25622	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.

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

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

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.

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 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 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-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
V1.4 (2022-10-11):	Added fix for SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants); removed SIMIT Simulation Platform as not affected
V1.5 (2022-12-13):	Added fix for SIMATIC S7-410 V10 CPU family and SIMATIC TDC
V1.6 (2023-01-10):	No fix planned for SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants), added fix for SINAMICS S120 (incl. SIPLUS variants)
V1.7 (2023-02-14):	Added additional SIMATIC ET200ecoPN products (CM 4x IO-Link, M12-L / CM 8x IO-Link, M12-L / AI 8xRTD/TC, M12-L) to the list of affected products
V1.8 (2023-04-11):	Added fix for SINAMICS G130, G150, S150
V1.9 (2023-07-11):	Added fix for SINAMICS G110M, G115D, G120; Expanded SIMATIC S7-400 V7 CPU family to individual products and MLFBs; clarified that no fix is planned for SIMATIC S7-400 PN/DP V7 CPUs, while other S7-400 V7 CPUs are not affected
V2.0 (2024-05-14):	Added fix for several SIMATIC ET200ecoPN devices
V2.1 (2024-06-11):	Added fix for SINAMICS S210, SIMATIC CFU DIQ and SIMATIC CFU PA
V2.2 (2024-07-09):	Added fix for SINAMICS DCM and SINAMICS V90; clarified that no fix is planned for SINAMICS S110; listed affected products individually instead of product families (e.g., for SIMATIC ET 200AL/MP/SP/pro IM families); added affected SIPLUS devices (e.g., SIPLUS ET 200xx IM)

TERMS OF USE