SSA-593272: SegmentSmack in Interniche IP-Stack based Industrial Devices

Publication Date: 2020-04-14
Last Update: 2024-05-14
Current Version: V2.1
CVSS v3.1 Base Score: 7.5

SUMMARY

A vulnerability exists in affected products that could allow remote attackers to affect the availability of the devices under certain conditions.

The underlying TCP stack can be forced to make very computation expensive calls for every incoming packet which can lead to a Denial-of-Service.

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 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: EK-ERTEC 200: All versions affected by all CVEs	Currently no fix is planned
Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P: All versions affected by all CVEs	Currently no fix is planned
KTK ATE530S: All versions affected by all CVEs	Currently no fix is planned
SIDOOR ATD430W: All versions affected by all CVEs	Currently no fix is planned
SIDOOR ATE530S COATED: All versions affected by all CVEs	Currently no fix is planned
SIDOOR ATE531S: All versions affected by all CVEs	Currently no fix is planned
SIMATIC ET200AL IM157-1 PN: All versions affected by all CVEs	Currently no fix is planned
SIMATIC ET200ecoPN, AI 8xRTD/TC, M12-L (6ES7144-6JF00-0BB0): All versions >= V5.1.1 < V5.1.2 affected by all CVEs	Update to V5.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109955667/

SIMATIC ET200ecoPN, CM 4x IO-Link, M12-L (6ES7148-6JE00-0BB0): All versions >= V5.1.1 affected by all CVEs	Currently no fix is planned
SIMATIC ET200ecoPN, CM 8x IO-Link, M12-L (6ES7148-6JG00-0BB0): All versions >= V5.1.1 affected by all CVEs	Currently no fix is planned
SIMATIC ET200ecoPN, CM 8x IO-Link, M12-L (6ES7148-6JJ00-0BB0): All versions >= V5.1.1 affected by all CVEs	Currently no fix is planned
SIMATIC ET200ecoPN, DI 8x24VDC, M12-L (6ES7141-6BG00-0BB0): All versions >= V5.1.1 < V5.1.2 affected by all CVEs	Update to V5.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109798525/
SIMATIC ET200ecoPN, DI 16x24VDC, M12-L (6ES7141-6BH00-0BB0): All versions >= V5.1.1 < V5.1.2 affected by all CVEs	Update to V5.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109798527/
SIMATIC ET200ecoPN, DIQ 16x24VDC/2A, M12-L (6ES7143-6BH00-0BB0): All versions >= V5.1.1 < V5.1.3 affected by all CVEs	Update to V5.1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109798530/
SIMATIC ET200ecoPN, DQ 8x24VDC/0,5A, M12-L (6ES7142-6BG00-0BB0): All versions >= V5.1.1 < V5.1.2 affected by all CVEs	Update to V5.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109798528/
SIMATIC ET200ecoPN, DQ 8x24VDC/2A, M12-L (6ES7142-6BR00-0BB0): All versions >= V5.1.1 < V5.1.2 affected by all CVEs	Update to V5.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109798529/
SIMATIC ET200MP IM155-5 PN HF (incl. SIPLUS variants): All versions >= V4.2 affected by all CVEs	Currently no fix is planned
SIMATIC ET200SP IM155-6 MF HF: All versions affected by all CVEs	Currently no fix is planned
SIMATIC ET200SP IM155-6 PN HA (incl. SIPLUS variants): All versions affected by all CVEs	Currently no fix is planned
SIMATIC ET200SP IM155-6 PN HF (incl. SIPLUS variants): All versions >= V4.2 affected by all CVEs	Currently no fix is planned

SIMATIC ET200SP IM155-6 PN/2 HF (incl. SIPLUS variants): All versions >= V4.2 affected by all CVEs	Currently no fix is planned
SIMATIC ET200SP IM155-6 PN/3 HF (incl. SIPLUS variants): All versions >= V4.2 affected by all CVEs	Currently no fix is planned
SIMATIC ET 200pro IM154-8 PN/DP CPU (6ES7154-8AB01-0AB0): All versions affected by all CVEs	Currently no fix is planned
SIMATIC ET 200pro IM154-8F PN/DP CPU (6ES7154-8FB01-0AB0): All versions affected by all CVEs	Currently no fix is planned
SIMATIC ET 200pro IM154-8FX PN/DP CPU (6ES7154-8FX00-0AB0): All versions affected by all CVEs	Currently no fix is planned
SIMATIC ET 200S IM151-8 PN/DP CPU (6ES7151-8AB01-0AB0): All versions affected by all CVEs	Currently no fix is planned
SIMATIC ET 200S IM151-8F PN/DP CPU (6ES7151-8FB01-0AB0): All versions affected by all CVEs	Currently no fix is planned
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions < V2.0 affected by all CVEs	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109759122/
SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants): All versions < V2.0 affected by all CVEs	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109759122/
SIMATIC MICRO-DRIVE PDC: All versions affected by all CVEs	Currently no fix is planned
SIMATIC PN/MF Coupler (6ES7158-3MU10-0XA0): All versions affected by all CVEs	Currently no fix is planned
SIMATIC PN/PN Coupler (6ES7158-3AD10-0XA0): All versions >= V4.2 affected by all CVEs	Currently no fix is planned

SIMATIC S7-300 CPU 314C-2 PN/DP (6ES7314-6EH04-0AB0): All versions affected by all CVEs	Currently no fix is planned As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SIMATIC S7-300 CPU 315-2 PN/DP (6ES7315-2EH14-0AB0): All versions affected by all CVEs	Currently no fix is planned As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SIMATIC S7-300 CPU 315F-2 PN/DP (6ES7315-2FJ14-0AB0): All versions affected by all CVEs	Currently no fix is planned As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SIMATIC S7-300 CPU 315T-3 PN/DP (6ES7315-7TJ10-0AB0): All versions affected by all CVEs	Currently no fix is planned As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SIMATIC S7-300 CPU 317-2 PN/DP (6ES7317-2EK14-0AB0): All versions affected by all CVEs	Currently no fix is planned As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SIMATIC S7-300 CPU 317F-2 PN/DP (6ES7317-2FK14-0AB0): All versions affected by all CVEs	Currently no fix is planned As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SIMATIC S7-300 CPU 317T-3 PN/DP (6ES7317-7TK10-0AB0): All versions affected by all CVEs	Currently no fix is planned As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SIMATIC S7-300 CPU 317TF-3 PN/DP (6ES7317-7UL10-0AB0): All versions affected by all CVEs	Currently no fix is planned As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SIMATIC S7-300 CPU 319-3 PN/DP (6ES7318-3EL01-0AB0): All versions affected by all CVEs	Currently no fix is planned As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SIMATIC S7-300 CPU 319F-3 PN/DP (6ES7318-3FL01-0AB0): All versions affected by all CVEs	Currently no fix is planned As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead

SIMATIC S7-400 H V6 CPU family and below (incl. SIPLUS variants): All versions affected by all CVEs	Currently no fix is planned As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants): All versions affected by all CVEs	Currently no fix is planned As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants): All versions affected by all CVEs	Currently no fix is available As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SIMATIC S7-410 V10 CPU family (incl. SIPLUS variants): All versions affected by all CVEs	Currently no fix is available As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions < V4.4.0 affected by all CVEs	Update to V4.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109793280/
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V2.0 affected by all CVEs	Update to V2.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109773807/
SIMATIC S7-1500 Software Controller: All versions < V2.0 affected by all CVEs	Update to V20.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109772864/
SIMATIC TDC CP51M1: All versions affected by all CVEs	Currently no fix is planned
SIMATIC TDC CPU555: All versions affected by all CVEs	Currently no fix is planned
SIMATIC WinAC RTX 2010 (6ES7671-0RC08-0YA0): All versions affected by all CVEs	Currently no fix is planned
SIMATIC WinAC RTX F 2010 (6ES7671-1RC08-0YA0): All versions affected by all CVEs	Currently no fix is planned
SINAMICS S/G Control Unit w. PROFINET: All versions affected by all CVEs	Currently no fix is planned

SIPLUS ET 200S IM151-8 PN/DP CPU (6AG1151-8AB01-7AB0): All versions affected by all CVEs	Currently no fix is planned
SIPLUS ET 200S IM151-8F PN/DP CPU (6AG1151-8FB01-2AB0): All versions affected by all CVEs	Currently no fix is planned
SIPLUS NET PN/PN Coupler (6AG2158-3AD10-4XA0): All versions >= V4.2 affected by all CVEs	Currently no fix is planned
SIPLUS S7-300 CPU 314C-2 PN/DP (6AG1314-6EH04-7AB0): All versions affected by all CVEs	Currently no fix is planned As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SIPLUS S7-300 CPU 315-2 PN/DP (6AG1315-2EH14-7AB0): All versions affected by all CVEs	Currently no fix is planned As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SIPLUS S7-300 CPU 315F-2 PN/DP (6AG1315-2FJ14-2AB0): All versions affected by all CVEs	Currently no fix is planned As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SIPLUS S7-300 CPU 317-2 PN/DP (6AG1317-2EK14-7AB0): All versions affected by all CVEs	Currently no fix is planned As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SIPLUS S7-300 CPU 317F-2 PN/DP (6AG1317-2FK14-2AB0): All versions affected by all CVEs	Currently no fix is planned As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead

WORKAROUNDS AND MITIGATIONS

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

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

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.

SIDOOR is an automatic door management system that offers diverse application options and benefits in elevator, industrial and railway applications.

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

SIMATIC ET 200SP Open Controller is a PC-based version of the SIMATIC S7-1500 Controller including optional visualization in combination with central I/Os in a compact device.

SIMATIC MICRO-DRIVE PDC are drive converters for servo drives in the protective extra low voltage range.

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

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

SIMATIC S7-1500 Software Controller is a SIMATIC software controller for PC-based automation solutions.

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.

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-2019-19300

The Interniche-based TCP Stack can be forced to make very expensive calls for every incoming packet which can lead to a denial of service.

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-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 (2020-04-14):	Publication Date
V1.1 (2020-05-12):	Added SIMATIC S7-400 H V6 CPU family and below to the list of affected products
V1.2 (2021-03-09):	Added Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200 (P) to the list of affected products
V1.3 (2022-02-08):	No remediation planned for SIMATIC ET200 devices
V1.4 (2022-03-11):	Added mitigation measure for SIMATIC S7-300 and S7-400
V1.5 (2022-03-28):	Updated fix and mitigation measures for SIMATIC S7-300 and S7-400
V1.6 (2022-04-12):	Cleanup due to template changes, no change of contents
V1.7 (2022-06-14):	Added SIMATIC S7-1200 CPU family, ET200SP/MP/AL/EcoPN and PN/xx Coupler to the list of affected products
V1.8 (2022-12-13):	Added fix for SIMATIC S7-410 CPU family (incl. SIPLUS variants)
V1.9 (2023-01-10):	Removed fix for SIMATIC S7-410 V10 CPU family (incl. SIPLUS variants) and added SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants) to the list of affected products
V2.0 (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
V2.1 (2024-05-14):	Added fix for several SIMATIC ET200ecoPN devices

TERMS OF USE