SSA-592007: Denial-of-Service Vulnerability in Industrial Products

Publication Date: 2018-03-20
Last Update: 2020-02-10
Current Version: V1.6
CVSS v3.1 Base Score: 5.3

SUMMARY

Several industrial controllers are affected by a security vulnerability that could allow an attacker to cause a Denial-of-Service condition via PROFINET DCP network packets under certain circumstances. Precondition for this scenario is a direct OSI Layer 2 access to the affected products. PROFIBUS interfaces are not affected.

Siemens has released updates for several affected products, is working on updates for the remaining affected products and recommends specific countermeasures until fixes are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
CP 343-1 Standard (incl. SIPLUS NET variants): All versions	See recommendations from section Workarounds and Mitigations
CP 443-1 Advanced (incl. SIPLUS NET variants) (incl. SIPLUS NET variants): All versions	See recommendations from section Workarounds and Mitigations
CP 443-1 Standard (incl. SIPLUS NET variants): All versions	See recommendations from section Workarounds and Mitigations
CP343-1 Advanced (incl. SIPLUS NET variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V1.7.0	Update to V1.8.5 or newer https://support.industry.siemens.com/cs/ww/en/view/109478459
SIMATIC S7-1500 Software Controller (incl. F): All versions < V1.7.0	Update to V1.8.5 or newer https://support.industry.siemens.com/cs/ww/en/view/109478528
SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V3.X.16	Update to V3.X.16 https://support.industry.siemens.com/cs/ww/en/ps/13752/dl
SIMATIC S7-400 H V6 CPU family (incl. SIPLUS variants): All versions < V6.0.9	Update to V6.0.9 https://support.industry.siemens.com/cs/ww/en/view/109474550
SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants): All versions < V6.0.7	Update to V6.0.7 https://support.industry.siemens.com/cs/ww/en/view/109474874

SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-410 CPU family (incl. SIPLUS variants): All versions < V8.1	Update to V8.1 or newer https://support.industry.siemens.com/cs/ww/en/view/109476571
SIMATIC WinAC RTX (F) 2010: All versions < SIMATIC WinAC RTX 2010 SP3	Update to SIMATIC WinAC RTX 2010 SP3 and apply BIOS and Microsoft Windows updates https://support.industry.siemens.com/cs/ww/en/view/109765109
SINUMERIK 828D: All versions < V4.7 SP6 HF1	Update to V4.7 SP6 HF1 SINUMERIK software can be obtained from your local Siemens account manager
Softnet PROFINET IO for PC-based Windows systems: 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:

- Apply cell protection concept: https://www.siemens.com/cert/operational-guidelines-industrial-security.
- Use VPN for protecting network communication between cells.
- Apply Defense-in-Depth: https://www.siemens.com/cert/operational-guidelines-industrial-security.

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

Communication Processor (CP) modules of families SIMATIC CP 343-1 and CP 443-1 have been designed to enable SIMATIC S7-300/S7-400 CPUs for Ethernet communication.

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.

Products of the SIMATIC S7-1500 CPU family 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 WinAC RTX (F) 2010 is a SIMATIC software controller for PC-based automation solutions.

SINUMERIK CNC offers automation solutions for the shop floor, job shops and large serial production environments.

Softnet PROFINET IO for PC-based Windows systems allows setting up open control solutions on standard PC hardware.

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 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-2018-4843

Responding to a PROFINET DCP request with a specially crafted PROFINET DCP packet could cause a Denial-of-Service condition of the requesting system.

The security vulnerability could be exploited by an attacker located on the same Ethernet segment (OSI Layer 2) as the targeted device. Successful exploitation requires no user interaction or privileges and impacts the availability of core functionality of the affected device. A manual restart is required to recover the system.

At the time of advisory publication no public exploitation of this security vulnerability is known. Siemens provides mitigations to resolve the security issue. PROFIBUS interfaces are not affected.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

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 (2018-03-20):	Publication Date
V1.1 (2018-03-27):	Removed SINUMERIK 840D sl from affected products
V1.2 (2018-10-09):	Added update for SINUMERIK 828D
V1.3 (2019-01-08):	Added update for SIMATIC S7-300 incl. F and T
V1.4 (2019-05-14):	Added update for S7-400 H V6
V1.5 (2019-10-08):	Renamed SIMATIC WinAC RTX 2010 incl. F to SIMATIC WinAC RTX (F) 2010 and added update information for SIMATIC WinAC RTX (F) 2010
V1.6 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products

TERMS OF USE