SSA-349422: Denial-of-Service in Industrial Real-Time (IRT) Devices

Publication Date: 2019-10-08
Last Update: 2020-08-11
Current Version: V1.4
CVSS v3.1 Base Score: 7.5

SUMMARY

A vulnerability in the affected products could allow an unauthorized attacker with network access to perform a denial-of-service attack resulting in loss of real-time synchronization.

Siemens has released updates for several affected products, and recommends that customers update to the new version. Siemens is preparing further updates and recommends specific countermeasures until updates are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller: All versions < V4.1.1 Patch 05	Update to V4.1.1 Patch 05 https://support.industry.siemens.com/cs/ww/en/view/109755160
Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200: All versions < V4.5.0 Patch 01	Update to V4.5.0 Patch 01 https://support.industry.siemens.com/cs/ww/en/view/109760397
Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P: All versions < V4.5.0	Update to V4.5.0 https://support.industry.siemens.com/cs/ww/en/view/109750012
SCALANCE X-200IRT switch family (incl. SIPLUS NET variants): All versions < V5.2.1	Update to V5.4.2 https://support.industry.siemens.com/cs/ww/en/view/109763309
SIMATIC ET200M (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET200S (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN (except 6ES7141-6BG00-0BB0, 6ES7141-6BH00-0BB0, 6ES7142-6BG00-0BB0, 6ES7142-6BR00-0BB0, 6ES7143-6BH00-0BB0, 6ES7146-6FF00-0AB0 and 6ES7148-6JD00-0AB0): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET200pro: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 1604: All versions < V2.8	Update to V2.8 https://support.industry.siemens.com/cs/ww/en/view/109762689

SIMATIC NET CP 1616: All versions < V2.8	Update to V2.8 https://support.industry.siemens.com/cs/ww/en/view/109762689
SIMATIC PN/PN Coupler 6ES7158-3AD01-0XA0 (incl. SIPLUS NET variant): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V3.X.17	Update to V3.X.17 https://support.industry.siemens.com/cs/ww/en/ps/13752/dl
SIMATIC S7-400 PN/DP V6 and below CPU family (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
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
SIMOTION (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SINAMICS DCM: All versions < V1.5 HF1	Update to V1.5 HF1 https://support.industry.siemens.com/cs/us/en/view/44029688
SINAMICS DCP: All versions < V1.3	Update to V1.3 https://support.industry.siemens.com/cs/ww/de/view/109773826
SINAMICS G110M V4.7 Control Unit: All versions < V4.7 SP10 HF5	Update to V4.7 SP10 HF5 https://support.industry.siemens.com/cs/us/en/view/109756820
SINAMICS G120 V4.7 Control Unit (incl. SIPLUS variants): All versions < V4.7 SP10 HF5	Update to V4.7 SP10 HF5 https://support.industry.siemens.com/cs/us/en/view/109756820
SINAMICS G130 V4.7 Control Unit: All versions < V4.7 HF29	Update to V4.7 HF29 or upgrade to V5.2 HF2 https://support.industry.siemens.com/cs/ww/en/view/103433117/
SINAMICS G150 Control Unit: All versions < V4.8	See recommendations from section Workarounds and Mitigations
SINAMICS GH150 V4.7 Control Unit: All versions	Upgrade to V4.8 SP2 HF9 The update can be obtained from your Siemens representative or via Siemens customer service.
SINAMICS GL150 V4.7 Control Unit: All versions	Upgrade to V4.8 SP2 HF9 The update can be obtained from your Siemens representative or via Siemens customer service.

SINAMICS GM150 V4.7 Control Unit: All versions	Upgrade to V4.8 SP2 HF9 The update can be obtained from your Siemens representative or via Siemens customer service.
SINAMICS S110 Control Unit: All versions	See recommendations from section Workarounds and Mitigations
SINAMICS S120 V4.7 Control Unit and CBE20 (incl. SIPLUS variants): All versions < V4.7 HF34	Update to V4.7 HF34 or upgrade to V5.2 HF2 https://support.industry.siemens.com/cs/us/en/view/92522512
SINAMICS S150 Control Unit: All versions < V4.8	See recommendations from section Workarounds and Mitigations
SINAMICS SL150 V4.7 Control Unit: All versions < V4.7 HF33	Update to V4.7 HF33 The update can be obtained from your Siemens representative or via Siemens customer service.
SINAMICS SM120 V4.7 Control Unit: All versions	See recommendations from section Workarounds and Mitigations
SINUMERIK 828D: All versions < V4.8 SP5	Update to V4.8 SP5 The update can be obtained from your Siemens representative or via Siemens customer service.
SINUMERIK 840D sl: 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:

- Restrict network access to port 161/udp of the affected product.
- Disable SNMP in Versions 1 and 2c, if supported by the product.
- Enable SNMP v3 if required and supported by the product to restrict the vulnerability to authenticated users.
- Enable access protection and change default credentials for SNMP service, if possible

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

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 WinAC RTX (F) 2010 is a SIMATIC software controller for PC-based automation solutions.

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

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

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

The SIMATIC NET CP 1616 and CP 1604 interface cards are used for connecting Personal Computers and PCI-104 systems to PROFINET IO.

SCALANCE X switches are used to connect industrial components like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs).

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-2019-10923

An attacker with network access to an affected product may cause a Denial-of-Service condition by breaking the real-time synchronization (IRT) of the affected installation.

The security vulnerability could be exploited by an unauthenticated attacker with network access to the affected installation. No user interaction is required to exploit this security vulnerability. The vulnerability impacts the availability of the affected installations.

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

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 (2019-10-08):	Publication Date
V1.1 (2020-01-14):	Added solution for SINAMICS SL150 V4.7, SIPLUS devices now explicitly mentioned in the list of affected products, correction in section “Workarounds and Mitigations”
V1.2 (2020-02-11):	Added solution for SINAMICS DCP
V1.3 (2020-03-10):	Added solution for SIMATIC S7-300 CPU family
V1.4 (2020-08-11):	Added SIMATIC ET200ecoPN product variants (MLFB IDs) that are not affected

TERMS OF USE