# SSA-473245: Denial-of-Service Vulnerability in Profinet Devices

Publication Date: 2019-10-08
Last Update: 2020-09-08
Current Version: V1.8
CVSS v3.1 Base Score: 7.5

## SUMMARY

A vulnerability in affected devices could allow an attacker to perform a denial-of-service attack if a large amount of specially crafted UDP packets are sent to the device.

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 patches are available.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller: All versions | See recommendations from section Workarounds and Mitigations |
| Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200: All versions | See recommendations from section Workarounds and Mitigations |
| Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P: All versions < V4.6 Patch 01 | Update to V4.6 Patch 01 https://support.industry.siemens.com/cs/ww/en/view/109781345 |
| SIMATIC CFU PA: All versions < V1.2.0 | Update to V1.2.0 https://support.industry.siemens.com/cs/ww/en/view/109754628 |
| SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants): All versions < V2.0 | Update to the latest version https://support.industry.siemens.com/cs/ww/en/view/109759122 |
| SIMATIC ET200AL: All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200M (incl. SIPLUS variants): All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200MP IM155-5 PN BA (incl. SIPLUS variants): All versions < V4.3.0 | Update to V4.3.0 https://support.industry.siemens.com/cs/ww/en/view/109754281 |
| SIMATIC ET200MP IM155-5 PN HF (incl. SIPLUS variants): All versions < V4.4.0 | Update to V4.4.0 https://support.industry.siemens.com/cs/ww/en/view/93012181 |

| | |
|---|---|
| SIMATIC ET200MP IM155-5 PN ST (incl. SIPLUS variants):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200S (incl. SIPLUS variants):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200SP IM155-6 PN BA (incl. SIPLUS variants):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200SP IM155-6 PN HA (incl. SIPLUS variants):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200SP IM155-6 PN HF (incl. SIPLUS variants):<br>All versions < V4.2.2 | Update to V4.2.2<br>https://support.industry.siemens.com/cs/ww/en/view/85624387 |
| SIMATIC ET200SP IM155-6 PN HS (incl. SIPLUS variants):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200SP IM155-6 PN ST (incl. SIPLUS variants):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200SP IM155-6 PN/2 HF (incl. SIPLUS variants):<br>All versions < V4.2.2 | Update to V4.2.2<br>https://support.industry.siemens.com/cs/ww/en/view/109769765 |
| SIMATIC ET200SP IM155-6 PN/3 HF (incl. SIPLUS variants):<br>All versions < V4.2.1 | Update to V4.2.1<br>https://support.industry.siemens.com/cs/ww/en/view/109769419 |
| 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):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200pro:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC HMI Comfort Outdoor Panels 7" & 15" (incl. SIPLUS variants):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC HMI Comfort Panels 4" - 22" (incl. SIPLUS variants):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC HMI KTP Mobile Panels:<br>All versions | See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC PN/PN Coupler (incl. SIPLUS NET variants):<br>All versions < V4.2.1 | Update to V4.2.1<br>https://support.industry.siemens.com/cs/ww/en/view/109760973 |
| SIMATIC PROFINET Driver:<br>All versions < V2.1 | Update to V2.1<br>https://support.industry.siemens.com/cs/ww/en/view/109768047 |
| SIMATIC S7-1200 CPU family (incl. SIPLUS variants):<br>All versions < V4.4.0 | Update to V4.4.0<br>https://support.industry.siemens.com/cs/ww/en/view/109763919 |
| SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants):<br>All versions < V2.0 | See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 Software Controller:<br>All versions < V2.0 | Update to the latest version<br>https://support.industry.siemens.com/cs/ww/en/view/109764666 |
| SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants):<br>All versions < V3.X.17 | Update to V3.X.17<br>https://support.industry.siemens.com/cs/ww/en/ps/13752/dl |
| SIMATIC S7-400 H V6 CPU family (incl. SIPLUS variants):<br>All versions < V6.0.9 | Update to V6.0.9<br>https://support.industry.siemens.com/cs/ww/en/view/109474550 |
| SIMATIC S7-400 PN/DP V6 and below CPU family (incl. SIPLUS variants):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants):<br>All versions < V8.2.2 | Update to V8.2.2<br>https://support.industry.siemens.com/cs/us/en/view/109476571 |
| SIMATIC TDC CP51M1:<br>All versions < V1.1.8 | Update to V1.1.8<br>https://support.industry.siemens.com/cs/ww/en/view/27049282 |
| SIMATIC TDC CPU555:<br>All versions < V1.1.1 | Update to V1.1.1<br>https://support.industry.siemens.com/cs/ww/en/view/109740119 |
| SIMATIC WinAC RTX (F) 2010:<br>All versions < SIMATIC WinAC RTX 2010 SP3 | Update to SIMATIC WinAC RTX 2010 SP3 and apply BIOS and Microsoft Windows updates<br>https://support.industry.siemens.com/cs/ww/en/view/109765109 |
| SINAMICS DCM:<br>All versions < V1.5 HF1 | Update to V1.5 HF1<br>https://support.industry.siemens.com/cs/ww/en/view/44029688 |

| | |
|---|---|
| SINAMICS DCP:<br>All versions < V1.3 | Update to V1.3<br>https://support.industry.siemens.com/cs/ww/en/view/109773826 |
| SINAMICS G110M V4.7 PN Control Unit:<br>All versions < V4.7 SP10 HF5 | Update to V4.7 SP10 HF5<br>https://support.industry.siemens.com/cs/ww/en/view/109756820 |
| SINAMICS G120 V4.7 PN Control Unit (incl. SIPLUS variants):<br>All versions < V4.7 SP10 HF5 | Update to V4.7 SP10 HF5<br>https://support.industry.siemens.com/cs/ww/en/view/109756820 |
| SINAMICS G130 V4.7 Control Unit:<br>All versions < 4.8 | Upgrade to V5.2 HF1<br>https://support.industry.siemens.com/cs/ww/en/view/109764679/ |
| SINAMICS G150 Control Unit:<br>All versions < 4.8 | Upgrade to V5.2 HF1<br>https://support.industry.siemens.com/cs/ww/en/view/109764679/ |
| SINAMICS GH150 V4.7 Control Unit:<br>All versions | Upgrade to V4.8 SP2 HF9<br>The update can be obtained from your Siemens representative or via Siemens customer service. |
| SINAMICS GL150 V4.7 Control Unit:<br>All versions | Upgrade to V4.8 SP2 HF9<br>The update can be obtained from your Siemens representative or via Siemens customer service. |
| SINAMICS GM150 V4.7 Control Unit:<br>All versions | Upgrade to V4.8 SP2 HF9<br>The update can be obtained from your Siemens representative or via Siemens customer service. |
| SINAMICS S110 Control Unit:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SINAMICS S120 V4.7 Control Unit (incl. SIPLUS variants):<br>All versions | Upgrade to V5.2 HF4<br>https://support.industry.siemens.com/cs/ww/en/view/109762626 |
| SINAMICS S150 Control Unit:<br>All versions < 4.8 | Upgrade to V5.2 HF1<br>https://support.industry.siemens.com/cs/ww/en/view/109764679/ |
| SINAMICS SL150 V4.7 Control Unit:<br>All versions < V4.7 HF33 | Update to V4.7 HF33<br>The update can be obtained from your Siemens representative or via Siemens customer service. |
| SINAMICS SM120 V4.7 Control Unit:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SINUMERIK 828D:<br>All versions < V4.8 SP5 | Update to V4.8 SP5<br>The update can be obtained from your Siemens representative or via Siemens customer service. |
| SINUMERIK 840D sl:<br>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 affected devices.

## 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

Siemens SIMATIC S7-300 CPU families, S7-400 CPU families, S7-1200 CPU families, and S7-1500 CPU families have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

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

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

PROFINET Driver is a development kit used to develop PROFINET IO controllers.

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

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

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

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.

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-2019-10936

Affected devices contain a vulnerability that allows an unauthenticated attacker to trigger a denial-of-service condition. The vulnerability can be triggered if a large amount of specially crafted UDP packets are sent to device.

The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the device.

At the time of advisory publication no public exploitation of this security vulnerability was known.

| | |
|---|---|
| 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 (2019-11-12): | Added solution for SINAMICS S120 V4.7, SINAMICS S150, SINAMICS G130 V4.7, SINAMICS G150 and SINAMICS SL150 V4.7 |
| V1.2 (2020-01-14): | Added solution for SIMATIC S7-1200 and S7-1500 Software and Open Controller. SIPLUS devices now explicitly mentioned in the list of affected products |
| V1.3 (2020-02-11): | Added solution for SINAMICS DCP |
| V1.4 (2020-03-10): | Added solution for SIMATIC S7-300 CPU family |
| V1.5 (2020-04-14): | Added solution for SIMATIC ET200MP IM155-5 PN HF |
| V1.6 (2020-07-14): | Added SIMATIC TDC CP51M1 and CPU555 to the list of affected products |
| V1.7 (2020-08-11): | Added solution for SIMATIC PN/PN Coupler. Added SIMATIC ET200ecoPN product variants (MLFB IDs) that are not affected |
| V1.8 (2020-09-08): | Added solution for EK-ERTEC 200P and S7-410 V8 |

## TERMS OF USE