# SSA-346262: Denial-of-Service in Industrial Products

| | |
|---|---|
| Publication Date: | 2017-11-23 |
| Last Update: | 2018-01-18 |
| Current Version: | V1.2 |
| CVSS v3.0 Base Score: | 7.5 |

## SUMMARY

Several industrial products are affected by a vulnerability that could allow remote attackers to conduct a Denial-of-Service (DoS) attack.

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 |
|---|---|
| SIMATIC S7-200 Smart:<br>All versions < V2.03.01 | Update to V2.03.01<br>https://support.industry.siemens.com/cs/cn/en/view/109749409 |
| SIMATIC S7-400 PN V6:<br>All versions < V6.0.6 | Update to V6.0.6<br>https://support.industry.siemens.com/cs/de/en/view/109474874 |
| SIMATIC S7-400 H V6:<br>All versions < V6.0.8 | Update to V6.0.8<br>https://support.industry.siemens.com/cs/ww/en/view/109474550 |
| SIMATIC S7-400 PN/DP V7:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-410 V8:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-300:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1200:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500:<br>All versions < V2.0 | Upgrade to V2.0 or newer<br>https://support.industry.siemens.com/cs/us/en/ps/13717/dl |
| SIMATIC S7-1500 Software Controller:<br>All versions < V2.0 | Upgrade to V2.0 or newer<br>https://support.industry.siemens.com/cs/us/en/view/109478528 |
| SIMATIC WinAC RTX 2010 incl. F:<br>All versions | See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC ET200AL:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200ecoPN:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200M:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200MP:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200pro:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200S:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200SP:<br>All versions | See recommendations from section Workarounds and Mitigations |
| Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller:<br>All versions | See recommendations from section Workarounds and Mitigations |
| Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P:<br>All versions < V4.5 | Update to V4.5<br>https://support.industry.siemens.com/cs/ww/en/view/31045047 |
| Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200 PN IO:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMOTION D:<br>All versions < V5.1 HF1 | Update to V5.1 HF1<br>https://support.industry.siemens.com/cs/ww/en/view/109750507 |
| SIMOTION C:<br>All versions < V5.1 HF1 | Update to V5.1 HF1<br>https://support.industry.siemens.com/cs/ww/en/view/31263919 |
| SIMOTION P:<br>All versions < V5.1 HF1 | Update to V5.1 HF1<br>Please contact your Siemens representative for information on how to obtain the update. |
| SINAMICS DCM:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SINAMICS DCP:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SINAMICS G110M w. PN:<br>All versions < V4.7 SP9 HF1 | Update to V4.7 SP9 HF1<br>https://support.industry.siemens.com/cs/document/109750507 |
| SINAMICS G120 (C/P/D) w. PN:<br>All versions < V4.7 SP9 HF1 | Update to V4.7 SP9 HF1<br>https://support.industry.siemens.com/cs/document/109750507 |

| | |
|---|---|
| SINAMICS G130 w. PN:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SINAMICS G150 w. PN:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SINAMICS S110 w. PN:<br>All versions < V4.4 SP3 HF6 | Update to V4.4 SP3 HF6<br>https://support.industry.siemens.com/cs/document/109474320 |
| SINAMICS S120 w. PN:<br>All versions < V4.8 HF5 | Update to V4.8 HF5<br>https://support.industry.siemens.com/cs/us/en/view/109740193 |
| SINAMICS S150 V4.7 w. PN:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SINAMICS S150 V4.8 w. PN:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SINAMICS V90 w. PN:<br>All versions < V1.02 | Update to V1.02<br>https://support.industry.siemens.com/cs/document/109746210 |
| SINUMERIK 840D sl:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC Compact Field Unit:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC PN/PN Coupler:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMOCODE pro V PROFINET:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIRIUS Soft Starter 3RW44 PN:<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:

- Disable SNMP if this is supported by the product (refer to the product documentation). Disabling SNMP fully mitigates the vulnerability.
- Protect network access to port 161/udp of affected devices.
- Apply cell protection concept and implement Defense-in-Depth: https://www.siemens.com/cert/operational-guidelines-industrial-security.
- Use VPN for protecting network communication between cells.

## GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to run the devices in a protected IT environment, Siemens particularly 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.

The SIMATIC Compact Field Unit is a field unit for use as an IO device on the PROFINET IO network 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.

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

The S7-200 SMART series is a line of micro-programmable logic controllers that can control a variety of small automation applications.

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 WinAC RTX is the SIMATIC software controller for PC-based automation solutions.

SIMOCODE pro is a flexible, modular motor management system for motors with constant speeds in the low-voltage performance range.

SIMOTION is a scalable high performance hardware and software system for motion control.

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.

SIRIUS 3RW soft starters permit soft starting and soft rampdown of three-phase asynchronous motors.

## VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

### Vulnerability (CVE-2017-12741)

Specially crafted packets sent to port 161/udp could cause a Denial-of-Service condition.The affected devices must be restarted manually.

| | |
|---|---|
| CVSS v3.0 Base Score | 7.5 |
| CVSS Vector | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |

## ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- George Lashenko from CyberX for coordinated disclosure of the vulnerability

## ADDITIONAL INFORMATION

For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

## HISTORY DATA

V1.0 (2017-11-23): Publication Date

V1.1 (2017-12-18): Changed affected products: V2.0 and newer of SIMATIC S7-1500 and V2.0 and newer of SIMATIC S7-1500 Software Controller are not affected. Added update information for SIMATIC S7-400 H V6

V1.2 (2018-01-18): New advisory format, added update information for SINAMICS V90 w. PN, SINAMICS S120 and SINAMICS S110 w. PN

## TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.