SSA-546832: Vulnerabilities in Medium Voltage SINAMICS and SIMOTION Products

Publication Date: 2018-05-03
Last Update: 2020-02-10
Current Version: V1.2
CVSS v3.1 Base Score: 7.5

SUMMARY

The latest updates for medium voltage SINAMICS products fix two security vulnerabilities that could allow an attacker to cause a Denial-of-Service condition either via specially crafted PROFINET DCP broadcast packets or by sending specially crafted packets to port 161/udp (SNMP). Precondition for the PROFINET DCP scenario is a direct Layer 2 access to the affected products. PROFIBUS interfaces are not affected.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMOTION D4xx V4.4 for SINAMICS SM150i-2 w. PROFINET (incl. SIPLUS variants): All versions < V4.4 HF26	Update to V4.4 HF26 The update can be obtained from your Siemens representative or via Siemens customer service.
SINAMICS GH150 V4.7 w. PROFINET: All versions < V4.7 SP5 HF7	Update to V4.7 SP5 HF7 or upgrade to V4.8 SP2 The update can be obtained from your Siemens representative or via Siemens customer service.
SINAMICS GL150 V4.7 w. PROFINET: All versions < V4.8 SP2	Upgrade to V4.8 SP2 The update can be obtained from your Siemens representative or via Siemens customer service.
SINAMICS GM150 V4.7 w. PROFINET: All versions < V4.7 HF31	Update to V4.7 HF31 or update to V4.8 SP2 The update can be obtained from your Siemens representative or via Siemens customer service.
SINAMICS SL150 V4.7.0 w. PROFINET: All versions < V4.7 HF30	Update to V4.7 HF30 or upgrade to V4.8 SP2 The update can be obtained from your Siemens representative or via Siemens customer service.
SINAMICS SL150 V4.7.4 w. PROFINET: All versions < V4.8 SP2	Upgrade to V4.8 SP2 The update can be obtained from your Siemens representative or via Siemens customer service.
SINAMICS SL150 V4.7.5 w. PROFINET: All versions < V4.8 SP2	Upgrade to V4.8 SP2 The update can be obtained from your Siemens representative or via Siemens customer service.
SINAMICS SM120 V4.7 w. PROFINET: All versions < V4.8 SP2	Upgrade to V4.8 SP2 The update can be obtained from your Siemens representative or via Siemens customer service.

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Apply cell protection concept and implement Defense-in-Depth: https://www.siemens.com/cert/operational-guidelines-industrial-security.
- Protect network access to port 161/udp of affected devices.
- 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 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

The SINAMICS medium voltage converter family is used to control a wide variety of medium voltage converters or inverters in different applications.

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-2017-2680

Specially crafted PROFINET DCP broadcast packets could cause a Denial-of-Service condition of affected products on a local Ethernet segment (Layer 2). Human interaction is required to recover the systems. PROFIBUS interfaces are not affected.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

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 v3.1 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 (‘Resource Exhaustion’)

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 (2018-05-03):	Publication Date
V1.1 (2018-10-09):	Clarified products name for SINAMICS SM150, and added update information; updated solution for SINAMICS GM150 V4.7 w. PROFINET
V1.2 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products

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.