SSA-606525: Denial-of-Service Vulnerability in SINAMICS PERFECT HARMONY GH180 Ethernet Modbus Interface (G28)

Publication Date: 2019-05-14
Last Update: 2019-05-14
Current Version: V1.0
CVSS v3.0 Base Score: 7.5

SUMMARY

SINAMICS PERFECT HARMONY GH180 Drives NXG I and NXG II control contains a denial-of-service vulnerability within the Ethernet Modbus interface (G28). An attacker with access to the Ethernet Modbus Interface could cause a Denial-of-Service condition exceeding the number of available connections.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINAMICS PERFECT HARMONY GH180 with NXG I control, MLFBs: 6SR2...-, 6SR3...-, 6SR4...-: All Versions with option G28	Upgrade to NXGpro control Please contact customer service to obtain and install the upgrade.
SINAMICS PERFECT HARMONY GH180 with NXG II control, MLFBs: 6SR2...-, 6SR3...-, 6SR4...-: All Versions with option G28	Upgrade to NXGpro control Please contact customer service to obtain and install the upgrade.

WORKAROUNDS AND MITIGATIONS

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

- Install a protocol bridge that isolates the networks and eliminates direct connections to the Ethernet modbus interface
- Apply cell protection concept and implement Defense-in-Depth

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), 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 Perfect Harmony GH180 medium voltage converter family is used to control a wide variety of medium voltage converters or inverters in different applications.

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-2019-6578

A denial of service vulnerability exists in the affected products.

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

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

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:W/RC:C

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 (2019-05-14): Publication Date

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.