

SSA-434535: Memory Protection Bypass Vulnerability in SINAMICS PERFECT HARMONY GH180 Drives

Publication Date: 2021-07-13
Last Update: 2021-07-13
Current Version: V1.0
CVSS v3.1 Base Score: 8.1

SUMMARY

Several models of SINAMICS PERFECT HARMONY GH180 Drives are affected by a memory protection bypass vulnerability in the integrated S7-1500 or S7-1200 CPU that could allow an attacker to write arbitrary data and code to protected memory areas or read sensitive data to launch further attacks on the CPU.

Siemens is preparing updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINAMICS PERFECT HARMONY GH180 Drives: 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:

- Avoid compromise of the individually configured access protection password to the S7-1500 or S7-1200 CPU
- Ensure that the drive internal network is not externally connected (which is the default configuration in all drives as described in the operational manual)

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 PERFECT HARMONY GH180 medium voltage drive 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 3.1 (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-2020-15782

Affected devices are vulnerable to a memory protection bypass through a specific operation.

A remote unauthenticated attacker with network access to port 102/tcp could potentially write arbitrary data and code to protected memory areas or read sensitive data to launch further attacks.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

ADDITIONAL INFORMATION

The following models of SINAMICS PERFECT HARMONY GH180 Drives are affected by CVE-2020-15782:

- 6SR5 with options A84, A85, E06, W41 with X30 air to air hex
- 6SR4 with option W41 with X30 air to air hex

For more information regarding CVE-2020-15782 refer to the Siemens Security Advisory SSA-434534 (<https://cert-portal.siemens.com/productcert/pdf/ssa-434534.pdf>)

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 (2021-07-13): 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.