SSA-910883: DHCP Client Vulnerability in SINAMICS PERFECT HARMONY GH180 Drives

Publication Date: 2022-07-12
Last Update: 2022-07-12
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

Several models of SINAMICS PERFECT HARMONY GH180 Drives are affected by a DHCP client vulnerability (CVE-2021-29998) in the integrated SCALANCE X206-1 device. The vulnerability could allow an attacker to cause a heap-based buffer overflow on that device and use it to get access to the drive's internal network.

The list of affected drive models can be found in the section "Additional Information" below.

Recently manufactured drives are no longer affected. For older drives, Siemens provides detailed remediation advise via customer support.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINAMICS PERFECT HARMONY GH180 Drives: Drives manufactured since 2015 and prior to 2022	Drives manufactured since 2022 are not affected Contact your Siemens customer support for detailed information how to remediate the issue in affected drives See further 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 the DHCP client and use static IP address configuration instead
- Ensure that the drive internal network is not externally connected (which is the default configuration in all drives as described in the operational manual)

Product specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

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-2021-29998

There is a DHCP vulnerability in Wind River VxWorks, for versions prior to 6.5. The vulnerability could cause a possible heap overflow if exploited.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

ADDITIONAL INFORMATION

The following models of SINAMICS PERFECT HARMONY GH180 Drives are affected by CVE-2021-29998:

- Water-cooled drives: all drives manufactured since 2015 and prior to February 2020
- Air-cooled drives: all drives manufactured since 2015 and prior to 2022, and with options G41 or G42 or with custom engineering

For more information regarding CVE-2021-29998 refer to the Siemens Security Advisory SSA-560465 (https://cert-portal.siemens.com/productcert/html/ssa-560465.html).

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 (2022-07-12): 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.