SSA-242353: Access Control Vulnerability in SINAMICS PERFECT HARMONY GH180

Publication Date: 2020-01-14
Last Update: 2020-01-14
Current Version: V1.0
CVSS v3.1 Base Score: 6.8

SUMMARY

A race condition in the restart behaviour of SINAMICS PERFECT HARMONY GH180 could allow an unauthorized attacker with physical access to the affected device to restart the HMI with disabled security controls, which could be used to launch further attacks against the affected device.

Siemens recommends customers to apply a configuration change on affected devices to resolve the issue. Detailed instructions are available through customer support.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINAMICS PERFECT HARMONY GH180 Drives MLFB 6SR32..-. . . .-. . . . MLFB 6SR4. . . -. . . .-. . . . MLFB 6SR5. . . -. . . .-. . . . With option A30 (HMIs 12 inches or larger): All versions	Apply the configuration changes as provided through customer support.
SINAMICS PERFECT HARMONY GH180 Drives MLFB 6SR325.-. . . .-. . . . (High Availability): All versions	Apply the configuration changes as provided through customer support.

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any specific mitigations or workarounds.

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 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 3.1 (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-2019-19278

The affected device contains a vulnerability that could allow an unauthenticated attacker to restore the affected device to a point where predefined application and operating system protection mechanisms are not in place.

Successful exploitation requires physical access to the system, but no system privileges and no user interaction. An attacker could use the vulnerability to compromise confidentialiy, integrity and availability of the device.

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

CVSS v3.1 Base Score	6.8
CVSS Vector	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-693: Protection Mechanism Failure

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 (2020-01-14): 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.