SSA-674165: Vulnerability in McAfee MACC product for SINAMICS PERFECT HARMONY GH180 drives

Publication Date: 2018-12-11
Last Update: 2018-12-11
Current Version: V1.0
CVSS v3.0 Base Score: 7.1

SUMMARY

McAfee has issued Security Bulletin SB10250 to address a vulnerabilty in McAfee Application and Change Control (MACC). SINAMICS PERFECT HARMONY GH180 Drives with HMIs produced between November 4th, 2015 and October 9th, 2018, use MACC as part of their software package, if option A30 was part of the order.

Siemens has analyzed the vulnerability and has determined that this vulnerability applies to these HMIs.

HMIs with this vulnerability can be compromised via local attack using removable USB storage devices to transfer malicious files. These file can be executed to compromise the HMI and by extension the drive system.

For compatibility reasons, Siemens advises the installation of MACC 8.2.0 instead of version 8.0.0, hotfix 5 as mentioned in SB10250.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINAMICS PERFECT HARMONY GH180 Drives: MLFB 6SR32..-. . . .-. . . . with option A30 (HMIs 12 inch or larger)	Upgrade to MACC V8.2.0 or greater using recommendations from McAfee https://kc.mcafee.com/corporate/index?page=content&id=SB10250
SINAMICS PERFECT HARMONY GH180 Drives: MLFB 6SR42..-. . . .-. . . . with option A30 (HMIs 12 inch or larger)	Upgrade to MACC V8.2.0 or greater using recommendations from McAfee https://kc.mcafee.com/corporate/index?page=content&id=SB10250
SINAMICS PERFECT HARMONY GH180 Drives: MLFB 6SR52..-. . . .-. . . . with option A30 (HMIs 12 inch or larger)	Upgrade to MACC V8.2.0 or greater using recommendations from McAfee https://kc.mcafee.com/corporate/index?page=content&id=SB10250
SINAMICS PERFECT HARMONY GH180 Drives: MLFB 6SR325..-. . . .-. . . . (High Availability)	Upgrade to MACC V8.2.0 or greater using recommendations from McAfee https://kc.mcafee.com/corporate/index?page=content&id=SB10250
SINAMICS PERFECT HARMONY GH180 Drives: MLFB 6SR32..-. . . .-. . . . with option A30 (HMIs 12 inch or larger) where the HMI is operating under Microsoft Windows XP	See recommendations from section Workarounds and Mitigations

SINAMICS PERFECT HARMONY GH180 Drives: MLFB 6SR42..-.....-.... with option A30 (HMIs 12 inch or larger) where the HMI is operating under Microsoft Windows XP	See recommendations from section Workarounds and Mitigations
SINAMICS PERFECT HARMONY GH180 Drives: MLFB 6SR52..-.....-.... with option A30 (HMIs 12 inch or larger) where the HMI is operating under Microsoft Windows XP	See recommendations from section Workarounds and Mitigations
SINAMICS PERFECT HARMONY GH180 Drives: MLFB 6SR325..-.....-.... (High Availability) where the HMI is operating under Microsoft Windows XP	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:

- Protect local access to the drive
- Ensure USB based storage media is blank and malware free before connecting to the drive
- 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: 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

SINAMICS PERFECT HARMONY GH180 is an air-cooled, medium-voltage drive for all kinds of industrial 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-2018-6690

The executable files from a hard drive solidified by MACC, of an external system, can be executed on the system that did not generate the inventory.

CVSS v3.0 Base Score	7.1
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- McAfee Corporation for publication of CVE-2018-6690

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 (2018-12-11): Publication Date

TERMS OF USE