SSA-742938: Open Ports in SINAMICS S/G Firmware

Publication Date: 2013-12-04
Last Update: 2020-02-10
Current Version: V1.3
CVSS v3.1 Base Score: 9.8

SUMMARY

A potential vulnerability was discovered in the SINAMICS S/G converter family which might allow attackers to access administrative functions on the device without authentication.

Siemens addresses the issue by a firmware update.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINAMICS G120 (incl. SIPLUS variants): All versions < V4.6 HF11	Update to V4.6 HF11 The firmware update can be obtained from your local Siemens account manager.

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 S/G converter family is used to control a wide variety of drives, especially in mechanical engineering and plant construction. They also interact with motion controllers, which are used among other things to coordinate synchronous operations or complex technology functions.

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

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-2013-6920

Open ports and services (FTP 21/tcp and Telnet 23/tcp) might allow attackers to access administrative functions of the affected devices over the network without authentication.

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-306: Missing Authentication for Critical Function

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

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 (2013-12-04):	Publication Date
V1.1 (2013-12-04):	Updated download information
V1.2 (2013-12-17):	Updated affected products (MLFBs) and firmware update version
V1.3 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products

TERMS OF USE