SSA-530931: Denial-of-Service in Webserver of Industrial Products

Publication Date: 2019-08-13
Last Update: 2020-05-12
Current Version: V1.3
CVSS v3.1 Base Score: 7.5

SUMMARY

A vulnerability in the affected products could allow an unauthorized attacker with network access to the webserver of an affected device to perform a denial-of-service attack.

Siemens has released updates for several affected products, and recommends that customers update to the new version. Siemens is preparing further updates and recommends specific countermeasures until patches are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINAMICS GH150 V4.7 (Control Unit): All versions	Upgrade to V4.8 SP2 HF9 or later version The software can be obtained from your Siemens representative or via Siemens customer service.
SINAMICS GH150 V4.8 (Control Unit): All versions < V4.8 SP2 HF9	Update to V4.8 SP2 HF9 or upgrade to later version The software can be obtained from your Siemens representative or via Siemens customer service.
SINAMICS GL150 V4.7 (Control Unit): All versions	Upgrade to V4.8 SP2 HF9 or later version The software can be obtained from your Siemens representative or via Siemens customer service.
SINAMICS GL150 V4.8 (Control Unit): All versions < V4.8 SP2 HF9	Update to V4.8 SP2 HF9 or upgrade to later version The software can be obtained from your Siemens representative or via Siemens customer service.
SINAMICS GM150 V4.7 (Control Unit): All versions	Upgrade to V4.8 SP2 HF9 or later version The software can be obtained from your Siemens representative or via Siemens customer service.
SINAMICS GM150 V4.8 (Control Unit): All versions < V4.8 SP2 HF9	Update to V4.8 SP2 HF9 or upgrade to later version The software can be obtained from your Siemens representative or via Siemens customer service.
SINAMICS SL150 V4.7 (Control Unit): All versions < V4.7 HF33	Update to V4.7 HF33 or upgrade to V5.2 SP2 The software can be obtained from your Siemens representative or via Siemens customer service.
SINAMICS SL150 V4.8 (Control Unit): All versions	Upgrade to V5.2 SP2 The software can be obtained from your Siemens representative or via Siemens customer service.
SINAMICS SM120 V4.7 (Control Unit): All versions	Upgrade to V4.8 SP2 HF10 or later version The software can be obtained from your Siemens representative or via Siemens customer service.

SINAMICS SM120 V4.8 (Control Unit): All versions < V4.8 SP2 HF10	Update to V4.8 SP2 HF10 or upgrade to later version The software can be obtained from your Siemens representative or via Siemens customer service.
SINAMICS SM150 V4.8 (Control Unit): All versions	Upgrade to V5.1 SP2 HF3 or later version The software can be obtained from your Siemens representative or via Siemens customer service.

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Apply appropriate strategies for mitigation as described in the General Security Recommendation section.
- Restrict network access to the integrated webserver.
- Deactivate the webserver if not required, and if deactivation is supported by the product. For SINAMICS products: Deactivate webserver with parameter P8986 = 0.

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 converter family is used to control a wide variety of drives, especially in mechanical engineering and plant construction.

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-2019-6568

The webserver of the affected devices contains a vulnerability that may lead to a denial-of-service condition. An attacker may cause a denial-of-service situation which leads to a restart of the webserver of the affected device.

The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the device.

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

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

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 (2019-08-13):	Publication Date
V1.1 (2019-11-12):	Added solution for SINAMICS SL150 V4.7
V1.2 (2019-12-10):	Added solution for SINAMICS SM120 V4.7 and SINAMICS SM120 V4.8
V1.3 (2020-05-12):	Added solution for SINAMICS SL150 V4.8

TERMS OF USE