

## SSA-752103: Telnet Authentication Vulnerability in SINAMICS Medium Voltage Products

Publication Date: 2021-05-11  
 Last Update: 2021-05-11  
 Current Version: V1.0  
 CVSS v3.1 Base Score: 8.1

### SUMMARY

SINAMICS medium voltage products, with telnet enabled on SIMATIC comfort HMI Panels, are affected by a remote access vulnerability that could allow an attacker, under certain conditions, to gain full remote access to the HMI. Note that by default telnet is disabled, but it can be enabled on request by the panel operator.

Siemens has released updates for some of the affected products, and recommends to update them to the latest version without undue delay. For the remaining affected products, Siemens is attempting to provide updates and recommends countermeasures (see recommendations from section Workarounds and Mitigations) for products where updates are not, or not yet available.

### AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINAMICS GH150: All versions	As only HMI image versions < V16 Update 3a are affected, please update the HMI Panel images as included in your installation of SINAMICS GH150 to V16 Update 4 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109746530/">https://support.industry.siemens.com/cs/ww/en/view/109746530/</a>
SINAMICS GL150 (with option X30): All versions	As only HMI image versions < V16 Update 3a are affected, please update the HMI Panel images as included in your installation of SINAMICS GL150 (with option X30) to V16 Update 4 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109746530/">https://support.industry.siemens.com/cs/ww/en/view/109746530/</a>
SINAMICS GM150 (with option X30): All versions	As only HMI image versions < V16 Update 3a are affected, please update the HMI Panel images as included in your installation of SINAMICS GM150 (with option X30) to V16 Update 4 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109746530/">https://support.industry.siemens.com/cs/ww/en/view/109746530/</a>
SINAMICS SH150: All versions	As only HMI image versions < V16 Update 3a are affected, please update the HMI Panel images as included in your installation of SINAMICS SH150 to V16 Update 4 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109746530/">https://support.industry.siemens.com/cs/ww/en/view/109746530/</a>
SINAMICS SL150: All versions	See recommendations from section <a href="#">Workarounds and Mitigations</a>

SINAMICS SM120: All versions	As only HMI image versions < V16 Update 3a are affected, please update the HMI Panel images as included in your installation of SINAMICS SM120 to V16 Update 4 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109746530/">https://support.industry.siemens.com/cs/ww/en/view/109746530/</a>
SINAMICS SM150: All versions	See recommendations from section <a href="#">Workarounds and Mitigations</a>
SINAMICS SM150i: All versions	See recommendations from section <a href="#">Workarounds and Mitigations</a>

## **WORKAROUNDS AND MITIGATIONS**

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

- Disable telnet on the HMI Panels if enabled. If this is not possible, [Defense-in-Depth](#) should be used. Note: By default telnet is disabled
- Follow [SINAMICS MV Industrial Security guidelines](#)

## **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 medium voltage converter family is used to control a wide variety of medium voltage converters or inverters in different applications.

SIMATIC HMI Panels are used for operator control and monitoring of machines and plants.

## **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-2020-15798

Affected devices with enabled telnet service do not require authentication for this service. This could allow a remote attacker to gain full access to the device. (ZDI-CAN-12046)

CVSS v3.1 Base Score	8.1
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C</a>
CWE	CWE-306: Missing Authentication for Critical Function

### **ADDITIONAL INFORMATION**

The CVSS score of the vulnerability listed in this advisory relates to the original affected HMI devices listed in [SSA-520004](#). The CVSS score for the products listed in this advisory is CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C (Base Score: 7.7).

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 (2021-05-11): 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](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.