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

Publication Date: 2021-05-11
Last Update: 2021-08-10
Current Version: V1.1
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 by the system integrator on request.

Siemens has released updates for the affected products, and recommends to update them to the latest version.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| SINAMICS GH150:<br>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<br>https://support.industry.siemens.com/cs/ww/en/view/109746530/ |
| SINAMICS GL150 (with option X30):<br>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<br>https://support.industry.siemens.com/cs/ww/en/view/109746530/ |
| SINAMICS GM150 (with option X30):<br>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<br>https://support.industry.siemens.com/cs/ww/en/view/109746530/ |
| SINAMICS SH150:<br>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<br>https://support.industry.siemens.com/cs/ww/en/view/109746530/ |
| SINAMICS SL150:<br>All versions | As only SIMATIC HMI image versions < V15 SP1 Update 6 are affected, please update the HMI Panel image as included in your installation of SINAMICS SL150 to V15 SP1 Update 6 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109763890/ |

  

| | |
|---|---|
| SINAMICS SM120:<br>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<br>https://support.industry.siemens.com/cs/ww/en/view/109746530/ |
| SINAMICS SM150:<br>All versions | https://support.industry.siemens.com/cs/ww/en/view/109763890/<br>As only SIMATIC HMI image versions < V15 SP1 Update 6 are affected, please update the HMI Panel image as included in your installation of SINAMICS SM150 to V15 SP1 Update 6 or later version |
| SINAMICS SM150i:<br>All versions | https://support.industry.siemens.com/cs/ww/en/view/109763890/<br>As only SIMATIC HMI image versions < V15 SP1 Update 6 are affected, please update the HMI Panel image as included in your installation of SINAMICS SM150i to V15 SP1 Update 6 or later version |

## WORKAROUNDS AND MITIGATIONS

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

- Follow SINAMICS MV Industrial Security guidelines
- 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, but it can be enabled by the system integrator on request.
- For any questions regarding update, please contact Siemens customer service or your system integrator.

## 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

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

The SINAMICS 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-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 | 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 |
| 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 |
| V1.1 (2021-08-10): | Updated information for SINAMICS SL150, SINAMICS SM150 and SINAMICS SM150i |

## TERMS OF USE