SSA-439673: Information Disclosure Vulnerability in SIPROTEC 5 Devices

Publication Date: 2022-01-11
Last Update: 2022-01-11
Current Version: V1.0
CVSS v3.1 Base Score: 6.5

SUMMARY

An information disclosure vulnerability in SIPROTEC 5 products could allow an unauthenticated attacker to read device information.

Only devices with the hardware variants CP050, CP100 and CP300 are affected. The DIGSI engineering tool can be used to identify the hardware version of your devices.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIPROTEC 5 6MD85 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 6MD86 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 6MD89 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 6MU85 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7KE85 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7SA82 devices (CPU variant CP100): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7SA86 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7SA87 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl

SIPROTEC 5 7SD82 devices (CPU variant CP100): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7SD86 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7SD87 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7SJ81 devices (CPU variant CP100): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7SJ82 devices (CPU variant CP100): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7SJ85 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7SJ86 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7SK82 devices (CPU variant CP100): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7SK85 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7SL82 devices (CPU variant CP100): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7SL86 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7SL87 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7SS85 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl

SIPROTEC 5 7ST85 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7SX85 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7UM85 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7UT82 devices (CPU variant CP100): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7UT85 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7UT86 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7UT87 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7VE85 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 7VK87 devices (CPU variant CP300): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl
SIPROTEC 5 Compact 7SX800 devices (CPU variant CP050): All versions < V8.83	Update to V8.83 or later version https://support.industry.siemens.com/cs/ww/en/ps/24237/dl

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific workarounds or mitigations. Please follow the General Security Recommendations.

Product specific mitigations can be found in the section Affected Products and Solution.

GENERAL SECURITY RECOMMENDATIONS

Operators of critical power systems (e.g. TSOs or DSOs) worldwide are usually required by regulations to build resilience into the power grids by applying multi-level redundant secondary protection schemes. It is therefore recommended that the operators check whether appropriate resilient protection measures are in place. The risk of cyber incidents impacting the grid's reliability can thus be minimized by virtue of the grid design.

Siemens strongly recommends applying the provided security updates using the corresponding tooling and documented procedures made available with the product. If supported by the product, an automated means to apply the security updates across multiple product instances may be used. Siemens strongly recommends prior validation of any security update before being applied, and supervision by trained staff of the update process in the target environment.

As a general security measure Siemens strongly recommends to protect network access with appropriate mechanisms (e.g. firewalls, segmentation, VPN). It is advised to configure the environment according to our operational guidelines in order to run the devices in a protected IT environment.

Recommended security guidelines to Digital Grid Products can be found at:

https://www.siemens.com/gridsecurity

PRODUCT DESCRIPTION

SIPROTEC 5 devices provide a range of integrated protection, control, measurement, and automation functions for electrical substations and other fields of application.

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-2021-41769

An improper input validation vulnerability in the web server could allow an unauthenticated user to access device information.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

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 (2022-01-11): Publication Date

TERMS OF USE