SSA-899560: Vulnerabilities in SIPROTEC 5 relays and DIGSI 5

Publication Date: 2019-07-09
Last Update: 2020-05-12
Current Version: V1.3
CVSS v3.1 Base Score: 7.5

SUMMARY

The SIPROTEC 5 relays and their corresponding engineering software DIGSI 5 are affected by two security vulnerabilities which could allow an attacker to upload or download files to the device or to conduct a Denial-of-Service attack over the network. Siemens has released updates for some affected products, is working on updates for the remaining affected products, and recommends specific countermeasures until fixes are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIPROTEC 5 device types 6MD85, 6MD86, 6MD89, 7UM85, 7SA87, 7SD87, 7SL87, 7VK87, 7SA82, 7SA86, 7SD82, 7SD86, 7SL82, 7SL86, 7SJ86, 7SK82, 7SK85, 7SJ82, 7SJ85, 7UT82, 7UT85, 7UT86, 7UT87 and 7VE85 with CPU variants CP300 and CP100 and the respective Ethernet communication modules: All versions < V7.90	Update to V7.90 or later version. Search for “SIPROTEC 5 - DIGSI Device Drivers” on the Siemens Industry Online Support site. The latest firmware version for the communication modules can also be found on each device specific download page. Applying the update causes the device / module to go through a single restart cycle. https://support.industry.siemens.com/cs/ww/en/
SIPROTEC 5 device types 7SS85 and 7KE85: All versions < V8.01	Update to V8.01 or later version. Search for “SIPROTEC 5 - DIGSI Device Drivers” on the Siemens Industry Online Support site. Applying the update causes the device / module to go through a single restart cycle. https://support.industry.siemens.com/cs/ww/en/
All other SIPROTEC 5 device types with CPU variants CP300 and CP100 and the respective Ethernet communication modules: All versions	See recommendations from section Workarounds and Mitigations
SIPROTEC 5 device types with CPU variants CP200 and the respective Ethernet communication modules: All versions < V7.59 only affected by CVE-2019-10931	Update to V7.59 or later version. Search for “SIPROTEC 5 - DIGSI Device Drivers” on the Siemens Industry Online Support site. The latest firmware version for the communication modules can also be found on each device specific download page. Applying the update causes the device / module to go through a single restart cycle. https://support.industry.siemens.com/cs/ww/en/

SIPROTEC 5 device types with CPU variants CP200 and the respective Ethernet communication modules: All versions only affected by CVE-2019-10930	See recommendations from section Workarounds and Mitigations
DIGSI 5 engineering software: All versions < V7.90	Update to V7.90 or later version and activate the client authorization feature https://support.industry.siemens.com/cs/us/en/view/109767686

WORKAROUNDS AND MITIGATIONS

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

- Block access to port 443/TCP e.g. with an external firewall.
- Activate role based access control (RBAC) in the device (supported in SIPROTEC 5 firmware versions V7.80 and higher)
- Activate the DIGSI 5 connection password in the device (supported in all SIPROTEC 5 firmware versions)

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

DIGSI 5 is the engineering and operating software for SIPROTEC 5 protection devices.

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-2019-10930

A remote attacker could use specially crafted packets sent to port 443/TCP to upload, download or delete files in certain parts of the file system.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-552: Files or Directories Accessible to External Parties

Vulnerability CVE-2019-10931

Specially crafted packets sent to port 443/TCP could cause a Denial of Service condition.

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-248: Uncaught Exception

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Pierre Capillon, Nicolas Iooss, and Jean-Baptiste Galet from Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) for coordinated disclosure

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 (2019-07-09):	Publication Date
V1.1 (2019-08-13):	Added further mitigations
V1.2 (2019-12-10):	Added update for SIPROTEC 5 device types with CPU variants CP200 and the respective Ethernet communication modules
V1.3 (2020-05-12):	Added update for SIPROTEC 5 device types 7SS85 and 7KE85

TERMS OF USE

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.