SSA-847986: Denial-of-Service Vulnerabilities in SIPROTEC 5 relays

Publication Date: 2021-09-14
Last Update: 2021-10-12
Current Version: V1.1
CVSS v3.1 Base Score: 9.8

SUMMARY

The latest update for SIPROTEC 5 relays fixes two vulnerabilities that could allow a remote attacker to cause a denial-of-service or potentially trigger a remote code execution under certain circumstances.

Siemens has released an update for SIPROTEC 5 relays and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIPROTEC 5 relays with CPU variants CP050: All versions < V8.80	Update to V8.80 or later version https://support.industry.siemens.com/cs/ww/en/view/109740816
SIPROTEC 5 relays with CPU variants CP100: All versions < V8.80	Update to V8.80 or later version https://support.industry.siemens.com/cs/ww/en/view/109740816
SIPROTEC 5 relays with CPU variants CP300: All versions < V8.80	Update to V8.80 or later version https://support.industry.siemens.com/cs/ww/en/view/109740816

WORKAROUNDS AND MITIGATIONS

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

- Block access to port 4443/tcp e.g. with an external firewall

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-2021-33719

Specially crafted packets sent to port 4443/tcp could cause a Denial-of-Service condition or potential remote code execution.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2021-33720

Specially crafted packets sent to port 4443/tcp could cause a Denial-of-Service condition.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Michael Messner from Siemens Energy for reporting the vulnerabilities

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 (2021-09-14): Publication Date
V1.1 (2021-10-12): Removed CP200 from list of affected products

TERMS OF USE