SSA-322980: Denial of Service Vulnerability in SIPROTEC 5 Devices

Publication Date: 2023-04-11
Last Update: 2024-05-14
Current Version: V1.4
CVSS v3.1 Base Score: 7.5

SUMMARY

SIPROTEC 5 devices contain a null pointer dereference vulnerability in the web service. This could allow an attacker to send unauthenticated maliciously crafted http request that could cause denial of service condition of the device.

Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIPROTEC 5 6MD85 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757428/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 6MD86 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757428/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 6MD89 (CP300): All versions >= V7.80 < V9.64 affected by all CVEs	Update to V9.64 or later version https://support.industry.siemens.com/cs/ww/en/view/109742950/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 6MU85 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109765263/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7KE85 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757430/ See further recommendations from section Workarounds and Mitigations

SIPROTEC 5 7SA82 (CP100): All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SA82 (CP150): All versions < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757433/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SA86 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757433/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SA87 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757433/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SD82 (CP100): All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SD82 (CP150): All versions < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757433/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SD86 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757433/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SD87 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757433/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SJ81 (CP100): All versions < V8.89 affected by all CVEs	Update to V8.89 or later V8.xx version https://support.industry.siemens.com/cs/ww/en/view/109751934/ See further recommendations from section Workarounds and Mitigations

SIPROTEC 5 7SJ81 (CP150): All versions < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109751934/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SJ82 (CP100): All versions < V8.89 affected by all CVEs	Update to V8.89 or later V8.xx version https://support.industry.siemens.com/cs/ww/en/view/109751934/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SJ82 (CP150): All versions < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109751934/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SJ85 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109751934/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SJ86 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757433/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SK82 (CP100): All versions < V8.89 affected by all CVEs	Update to V8.89 or later V8.xx version https://support.industry.siemens.com/cs/ww/en/view/109757434/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SK82 (CP150): All versions < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757434/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SK85 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757434/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SL82 (CP100): All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations

SIPROTEC 5 7SL82 (CP150): All versions < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757433/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SL86 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757433/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SL87 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757433/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SS85 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757429/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7ST85 (CP300): All versions >= V7.80 < V9.64 affected by all CVEs	Update to V9.64 or later version https://support.industry.siemens.com/cs/ww/en/view/109740299/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7ST86 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109768428/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SX82 (CP150): All versions < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109768011/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SX85 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109768011/ See further recommendations from section Workarounds and Mitigations

SIPROTEC 5 7UM85 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757431/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7UT82 (CP100): All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7UT82 (CP150): All versions < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757438/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7UT85 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757438/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7UT86 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757438/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7UT87 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757438/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7VE85 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109749865/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7VK87 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109757433/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7VU85 (CP300): All versions >= V7.80 < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109800399/ See further recommendations from section Workarounds and Mitigations

SIPROTEC 5 Communication Module ETH-BA-2EL: All versions < V9.40 installed on CP150 and CP300 devices affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109740816/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 Communication Module ETH-BA-2EL: All versions < V8.89 installed on CP100 devices affected by all CVEs	Update to V8.89 or later V8.xx version https://support.industry.siemens.com/cs/ww/en/view/109740816/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 Communication Module ETH-BB-2FO: All versions < V9.40 installed on CP150 and CP300 devices affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109740816/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 Communication Module ETH-BB-2FO: All versions < V8.89 installed on CP100 devices affected by all CVEs	Update to V8.89 or later V8.xx version https://support.industry.siemens.com/cs/ww/en/view/109740816/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 Communication Module ETH-BD-2FO: All versions < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109740816/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 Compact 7SX800 (CP050): All versions < V9.40 affected by all CVEs	Update to V9.40 or later version https://support.industry.siemens.com/cs/ww/en/view/109796884/ See further recommendations from section Workarounds and Mitigations

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
- Disable web service using port 4443 for SIPROTEC 5 if it is not needed

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

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 can be found at: https://www.siemens.com/gridsecurity

PRODUCT DESCRIPTION

SIPROTEC 5 and SIPROTEC 4 devices provide a range of integrated protection, control, measurement, and automation functions for electrical substations and other fields of application.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2023-28766

Affected devices lack proper validation of http request parameters of the hosted web service. An unauthenticated remote attacker could send specially crafted packets that could cause denial of service condition of the target device.

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-476: NULL Pointer Dereference

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Turek Witold from Polskie Sieci Elektroenergetyczne S.A for reporting the vulnerability

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 (2023-04-11): Publication Date

V1.1 (2023-05-09): Removed all non-impacted CP200 devices; added introduced version to CP300 devices; added additional mitigation measure

V1.2 (2023-09-12): Added fix for SIPROTEC 5 6MD89 (CP300) and SIPROTEC 5 7ST85 (CP300)

V1.3 (2024-03-12): Adjusted fix version for SIPROTEC 5 6MD89 (CP300) and SIPROTEC 5 7ST85 (CP300)

V1.4 (2024-05-14): Added fix for SIPROTEC 5 7SJ81 (CP100), SIPROTEC 5 7SJ82 (CP100), SIPROTEC 5 7SK82 (CP100), SIPROTEC 5 Communication Module ETH-BA-2EL (installed on CP100 devices), SIPROTEC 5 Communication Module ETH-BB-2FO (installed on CP100 devices); Clarified that currently no fix is available for SIPROTEC 5 7SA82 (CP100), SIPROTEC 5 7SD82 (CP100), SIPROTEC 5 7SL82 (CP100), SIPROTEC 5 7UT82 (CP100)

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, 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.