SSA-750499: Weak Encryption Vulnerability in SIPROTEC 5 Devices

Publication Date: 2024-07-09
Last Update: 2024-07-09
Current Version: V1.0
CVSS v3.1 Base Score: 5.9
CVSS v4.0 Base Score: 8.2

SUMMARY

The SIPROTEC 5 devices are supporting weak encryption. This could allow an unauthorized attacker in a man-in-the-middle position to read any data passed over the connection between legitimate clients and the affected 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 - CP050 Devices:	Update to V9.64 or later version https://support.industry.siemens.com/cs/ww/en/view/109796884/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 Compact 7SX800 (CP050): All versions < V9.64 affected by CVE-2024-38867	Update to V9.64 or later version https://support.industry.siemens.com/cs/ww/en/view/109796884/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 - CP100 Devices:	See below See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SA82 (CP100): All versions affected by CVE-2024-38867	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SD82 (CP100): All versions affected by CVE-2024-38867	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SJ81 (CP100): All versions < V8.89 affected by CVE-2024-38867	Update to V8.89 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 CVE-2024-38867	Update to V8.89 or later version https://support.industry.siemens.com/cs/ww/en/view/109751934/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SK82 (CP100): All versions < V8.89 affected by CVE-2024-38867	Update to V8.89 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 CVE-2024-38867	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7UT82 (CP100): All versions affected by CVE-2024-38867	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPROTEC 5 - CP150 Devices:	Update to V9.65 or later version See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SA82 (CP150): All versions < V9.65 affected by CVE-2024-38867	Update to V9.65 or later version https://support.industry.siemens.com/cs/ww/en/view/109757433/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SD82 (CP150): All versions < V9.65 affected by CVE-2024-38867	Update to V9.65 or later version https://support.industry.siemens.com/cs/ww/en/view/109757433/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SJ81 (CP150): All versions < V9.65 affected by CVE-2024-38867	Update to V9.65 or later 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 < V9.65 affected by CVE-2024-38867	Update to V9.65 or later version https://support.industry.siemens.com/cs/ww/en/view/109751934/ See further recommendations from section Workarounds and Mitigations

SIPROTEC 5 7SK82 (CP150): All versions < V9.65 affected by CVE-2024-38867	Update to V9.65 or later version https://support.industry.siemens.com/cs/ww/en/view/109757434/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SL82 (CP150): All versions < V9.65 affected by CVE-2024-38867	Update to V9.65 or later version https://support.industry.siemens.com/cs/ww/en/view/109757433/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SX82 (CP150): All versions < V9.65 affected by CVE-2024-38867	Update to V9.65 or later version https://support.industry.siemens.com/cs/ww/en/view/109768011/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7UT82 (CP150): All versions < V9.65 affected by CVE-2024-38867	Update to V9.65 or later version https://support.industry.siemens.com/cs/ww/en/view/109757438/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 - CP200 Devices:	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 6MD85 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 6MD86 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7KE85 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SA84 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SA86 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SA87 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIPROTEC 5 7SD84 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SD86 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SD87 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SJ85 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SJ86 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SK85 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SL86 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SL87 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SS85 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7ST85 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7UT85 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7UT86 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIPROTEC 5 7UT87 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 7VK87 (CP200): All versions affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 - CP300 Devices:	See below See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 6MD84 (CP300): All versions < V9.64 affected by CVE-2024-38867	Update to V9.64 or later version https://support.industry.siemens.com/cs/ww/en/view/109814150/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 6MD85 (CP300): All versions < V9.64 affected by CVE-2024-38867	Update to V9.64 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 < V9.64 affected by CVE-2024-38867	Update to V9.64 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 < V9.64 affected by CVE-2024-38867	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 < V9.64 affected by CVE-2024-38867	Update to V9.64 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 < V9.64 affected by CVE-2024-38867	Update to V9.64 or later version https://support.industry.siemens.com/cs/ww/en/view/109757430/ See further recommendations from section Workarounds and Mitigations

SIPROTEC 5 7SA86 (CP300): All versions < V9.65 affected by CVE-2024-38867	Update to V9.65 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 < V9.65 affected by CVE-2024-38867	Update to V9.65 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 < V9.65 affected by CVE-2024-38867	Update to V9.65 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 < V9.65 affected by CVE-2024-38867	Update to V9.65 or later version https://support.industry.siemens.com/cs/ww/en/view/109757433/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SJ85 (CP300): All versions < V9.65 affected by CVE-2024-38867	Update to V9.65 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 < V9.65 affected by CVE-2024-38867	Update to V9.65 or later version https://support.industry.siemens.com/cs/ww/en/view/109757433/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SK85 (CP300): All versions < V9.65 affected by CVE-2024-38867	Update to V9.65 or later version https://support.industry.siemens.com/cs/ww/en/view/109757434/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SL86 (CP300): All versions < V9.65 affected by CVE-2024-38867	Update to V9.65 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 < V9.65 affected by CVE-2024-38867	Update to V9.65 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 < V9.64 affected by CVE-2024-38867	Update to V9.64 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 < V9.64 affected by CVE-2024-38867	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 < V9.64 affected by CVE-2024-38867	Update to V9.64 or later version https://support.industry.siemens.com/cs/ww/en/view/109768428/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7SX85 (CP300): All versions < V9.65 affected by CVE-2024-38867	Update to V9.65 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 < V9.64 affected by CVE-2024-38867	Update to V9.64 or later version https://support.industry.siemens.com/cs/ww/en/view/109757431/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 7UT85 (CP300): All versions < V9.65 affected by CVE-2024-38867	Update to V9.65 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 < V9.65 affected by CVE-2024-38867	Update to V9.65 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 < V9.65 affected by CVE-2024-38867	Update to V9.65 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 < V9.64 affected by CVE-2024-38867	Update to V9.64 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 < V9.65 affected by CVE-2024-38867	Update to V9.65 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 < V9.64 affected by CVE-2024-38867	Update to V9.64 or later version https://support.industry.siemens.com/cs/ww/en/view/109800399/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 Communication Modules:	See below See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 Communication Module ETH-BA-2EL (Rev.1):	See below See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 Communication Module ETH-BA-2EL (Rev.1): All versions installed on CP200 devices affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 Communication Module ETH-BA-2EL (Rev.1): All versions < V8.89 installed on CP100 devices affected by CVE-2024-38867	Update to V8.89 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 (Rev.1): All versions < V9.62 installed on CP150 and CP300 devices affected by CVE-2024-38867	Update to V9.62 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 (Rev. 1):	See below See recommendations from section Workarounds and Mitigations

SIPROTEC 5 Communication Module ETH-BB-2FO (Rev. 1): All versions installed on CP200 devices affected by CVE-2024-38867	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 Communication Module ETH-BB-2FO (Rev. 1): All versions < V8.89 installed on CP100 devices affected by CVE-2024-38867	Update to V8.89 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 (Rev. 1): All versions < V9.62 installed on CP150 and CP300 devices affected by CVE-2024-38867	Update to V9.62 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-BD-2FO: All versions < V9.62 affected by CVE-2024-38867	Update to V9.62 or later version https://support.industry.siemens.com/cs/ww/en/view/109740816/ 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:

- Restrict access to port 443/tcp for web, 4443/tcp for DIGSI 5 and configurable port for syslog over TLS to trusted IP addresses only

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 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-2024-38867

The affected devices are supporting weak ciphers on several ports (443/tcp for web, 4443/tcp for DIGSI 5 and configurable port for syslog over TLS). This could allow an unauthorized attacker in a man-in-the-middle position to read and modify any data passed over to and from those ports.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS v4.0 Base Score	8.2
CVSS Vector	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
CWE	CWE-326: Inadequate Encryption Strength

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Hydro-Québec for coordinated disclosure of CVE-2024-38867

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 (2024-07-09): Publication Date

TERMS OF USE