SSA-726834: Denial of Service Vulnerability in the RADIUS Client of SIPROTEC 5 Devices

Publication Date: 2023-03-14
Last Update: 2023-03-14
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

The RADIUS client implementation of the VxWorks platform in SIPROTEC 5 devices contains a denial of service vulnerability that could be triggered when a specially crafted packet is sent by a RADIUS server.

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 (CP300): All versions >= V7.80 < V9.30	Update to V9.30 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 < V9.30	Update to V9.30 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	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPROTEC 5 6MU85 (CP300): All versions >= V7.90 < V9.30	Update to V9.30 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 < V9.30	Update to V9.30 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 >= V7.80 < V9.30	Update to V9.30 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 < V9.30	Update to V9.30 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 < V9.30	Update to V9.30 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 < V9.30	Update to V9.30 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 >= V7.80 < V9.30	Update to V9.30 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 < V9.30	Update to V9.30 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 >= V7.80 < V9.30	Update to V9.30 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 >= V7.80 < V9.30	Update to V9.30 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 < V9.30	Update to V9.30 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 < V9.30	Update to V9.30 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 >= V8.81 < V9.30	Update to V9.30 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 >= V9.20 < V9.30	Update to V9.30 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 >= V8.30 < V9.30	Update to V9.30 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 < V9.30	Update to V9.30 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 >= V7.80 < V9.30	Update to V9.30 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 < V9.30	Update to V9.30 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 < V9.30	Update to V9.30 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 < V9.30	Update to V9.30 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 < V9.30	Update to V9.30 or later version https://support.industry.siemens.com/cs/ww/en/view/109757433/ See further recommendations from section Workarounds and Mitigations
SIPROTEC 5 Communication Module ETH-BA-2EL: All versions >= V7.80 < V9.30	Update to V9.30 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 >= V7.80 < V9.30	Update to V9.30 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 >= V7.80 < V9.30	Update to V9.30 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 >= V8.70 < V9.30	Update to V9.30 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:

- Ensure that only a trusted, properly hardened RADIUS server is configured in your environment
- Protect the pre-shared key for RADIUS from unauthorized access

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 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-2022-38767

An issue was discovered in Wind River VxWorks 6.9 and 7, that allows a specifically crafted packet sent by a Radius server, may cause Denial of Service during the IP Radius access procedure.

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-835: Loop with Unreachable Exit Condition ('Infinite Loop')

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 (2023-03-14):   Publication Date

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.