

SSA-541017: Embedded TCP/IP Stack Vulnerabilities (AMNESIA:33) in SIRIUS 3RW5 Modbus TCP and SENTRON PAC / 3VA Devices

Publication Date: 2020-12-08
Last Update: 2021-04-13
Current Version: V1.3
CVSS v3.1 Base Score: 6.5

SUMMARY

Security researchers discovered and disclosed 33 vulnerabilities in several open-source TCP/IP stacks for embedded devices, also known as “AMNESIA:33” vulnerabilities.

This advisory describes the impact of one of these vulnerabilities (CVE-2020-13988) to Siemens products. Siemens has released updates for the affected products and recommends to update to the latest versions.

The impact of additional “AMNESIA:33” vulnerabilities is described in [Siemens Security Advisory SSA-541018](#).

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SENTRON 3VA COM100/800: All versions < V4.2	Update to V4.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109765343/
SENTRON 3VA DSP800: All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109761031/
SENTRON PAC2200 (without MID Approval): All versions < V3.0.5	Update to V3.0.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109760897/
SENTRON PAC3200: All versions < V2.4.5	Update to V2.4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/31674577/
SENTRON PAC3200T: All versions < V3.0.5	Update to V3.0.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109793060/
SENTRON PAC4200: All versions < V2.0.1	Update to V2.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/35029840/
SIRIUS 3RW5 communication module Modbus TCP: All versions < V1.1.1	Update to V1.1.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109759671/

WORKAROUNDS AND MITIGATIONS

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

- For successful exploitation, an attacking system must be located in the same Modbus TCP segment as a vulnerable device. Therefore ensure that only trusted systems are attached to that segment

and only trusted persons have access.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: <https://www.siemens.com/cert/operational-guidelines-industrial-security>), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: <https://www.siemens.com/industrialsecurity>

PRODUCT DESCRIPTION

SENTRON PAC Meter products are power measuring devices for precise energy management and transparent information acquisition.

The SENTRON 3VA DSP800 display device is used to display values retrieved from 3VA MCCB (Molded Case Circuit Breaker) devices.

The SENTRON 3VA COM100/COM800 breaker data server is used as a gateway and enables communication between 3VA MCCB (Molded Case Circuit Breaker) devices and automation systems.

SIRIUS 3RW soft starters permit soft starting and soft rampdown of three-phase asynchronous motors.

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-2020-13988

The TCP/IP stack (uIP) in affected devices is vulnerable to integer overflow when processing TCP Maximum Segment Size (MSS) options. (FSCT-2020-0008)

An attacker located in the same network could trigger a Denial-of-Service condition on the device by sending a specially crafted IP packet.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Jos Wetzels, Stanislav Dashevskyi, Amine Amri, and Daniel dos Santos from Forescout Technologies for coordinated disclosure
- Cybersecurity and Infrastructure Security Agency (CISA) for coordination efforts

- CERT Coordination Center (CERT/CC) for coordination efforts

ADDITIONAL INFORMATION

Impact of other “AMNESIA:33” vulnerabilities to Siemens products:

- [Siemens Security Advisory SSA-541018](#)

For more details regarding the AMNESIA:33 vulnerabilities in embedded TCP/IP stacks refer to:

- [Forescout Publication “AMNESIA:33”](#)
- [CERT/CC Advisory VU#815128](#)
- [CISA Industrial Control Systems Advisory ICSA-20-343-01](#)

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 (2020-12-08):	Publication Date
V1.1 (2021-02-09):	Added additional affected products (SENTRON PAC2200, PAC3200T, 3VA COM100/800, 3VA DSP800) and related fix release information
V1.2 (2021-03-09):	Added solution for SIRIUS 3RW5 communication module Modbus TCP; added reference to additional AMNESIA:33 advisory (SSA-541018)
V1.3 (2021-04-13):	Added download link for SENTRON PAC3200T

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.