# SSA-541018: Embedded TCP/IP Stack Vulnerabilities (AMNESIA:33) in SENTRON PAC / 3VA Devices (Part 2)

Publication Date: 2021-03-09
Last Update: 2021-03-09
Current Version: V1.0
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 two of these vulnerabilities (CVE-2020-13987, CVE-2020-17437) to Siemens products.

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

The impact of another “AMNESIA:33” vulnerability (CVE-2020-13988) is described in Siemens Security Advisory SSA-541017.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| SENTRON 3VA COM100/800:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SENTRON 3VA DSP800:<br>All versions<br>only affected by CVE-2020-17437 | See recommendations from section Workarounds and Mitigations |
| SENTRON PAC2200 (with CLP Approval):<br>All versions<br>only affected by CVE-2020-17437 | See recommendations from section Workarounds and Mitigations |
| SENTRON PAC2200 (with MID Approval):<br>All versions<br>only affected by CVE-2020-17437 | See recommendations from section Workarounds and Mitigations |
| SENTRON PAC2200 (without MID Approval):<br>All versions<br>only affected by CVE-2020-17437 | See recommendations from section Workarounds and Mitigations |
| SENTRON PAC3200:<br>All versions < V2.4.7 | Update to V2.4.7 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/31674577/ |
| SENTRON PAC3200T:<br>All versions<br>only affected by CVE-2020-17437 | See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SENTRON PAC3220:<br>All versions < V3.2.0<br>only affected by CVE-2020-17437 | Update to V3.2.0 or later version<br>Contact Siemens customer support to receive the latest firmware version. |
| SENTRON PAC4200:<br>All versions < V2.3.0 | Update to V2.3.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/35029840/ |

## 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.

## 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-2020-13987

The TCP/IP stack (uIP) in affected devices is vulnerable to out-of-bounds read when calculating the checksum for IP packets. (FSCT-2020-0009)

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-125: Out-of-bounds Read |

### Vulnerability CVE-2020-17437

The TCP/IP stack (uIP) in affected devices is vulnerable to out-of-bounds write when processing TCP packets with urgent pointer (URG) where the location of the TCP data payload is calculated improperly. (FSCT-2020-0018)

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-787: Out-of-bounds Write |

## 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-541017

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 (2021-03-09): Publication Date

## TERMS OF USE