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

Publication Date: 2020-12-08
Last Update: 2020-12-08
Current Version: V1.0
CVSS v3.1 Base Score: 6.5

SUMMARY

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

The Siemens products mentioned below are affected by one of these vulnerabilities (CVE-2020-13988).

Siemens has released updates for SENTRON PAC devices, is working on updates for SIRIUS 3RW5 communication module Modbus TCP, and recommends specific countermeasures for vulnerable product versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
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 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	See 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:

- 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.

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 due 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
- Industrial Control System Cyber Emergency Response Team (ICS-CERT) for coordination efforts
- CERT Coordination Center (CERT/CC) for coordination efforts

ADDITIONAL INFORMATION

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

TERMS OF USE