SSA-789208: Multiple Vulnerabilities (INFRA:HALT) in Interniche IP-Stack based Low Voltage Devices

Publication Date: 2021-08-04
Last Update: 2022-01-11
Current Version: V1.2
CVSS v3.1 Base Score: 7.5

SUMMARY

Security researchers discovered and disclosed 14 vulnerabilities in the Interniche IP stack, also known as “INFRA:HALT” vulnerabilities [0]. This advisory describes the impact to Siemens low voltage products, which are only affected by four out of the 14 vulnerabilities.

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

[0] https://www.forescout.com/blog/new-critical-operational-technology-vulnerabilities-found-on-nichestack/

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SENTRON 3WA COM190: All versions < V2.0.0 only affected by CVE-2020-35684, CVE-2020-35685, CVE-2021-31401	Update to V2.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109782123/
SENTRON 3WL COM35: All versions < V1.2.0 only affected by CVE-2020-35684, CVE-2020-35685, CVE-2021-31401	Update to V1.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109766651/
SENTRON 7KM PAC Switched Ethernet PROFINET Expansion Module (7KM9300-0AE00-0AA0): All versions only affected by CVE-2020-35683, CVE-2020-35684, CVE-2020-35685, CVE-2021-31401	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SENTRON 7KM PAC Switched Ethernet PROFINET Expansion Module (7KM9300-0AE01-0AA0): All versions < V2.1.6 only affected by CVE-2020-35683, CVE-2020-35684, CVE-2020-35685, CVE-2021-31401	Update to V2.1.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109749555/

SENTRON 7KM PAC Switched Ethernet PROFINET Expansion Module (7KM9300-0AE02-0AA0): All versions < V3.0.4 only affected by CVE-2020-35683, CVE-2020-35684, CVE-2020-35685, CVE-2021-31401	Update to V3.0.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109777120/

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific workarounds or mitigations. Please follow the General Security Recommendations.

Product specific mitigations can be found in the section Affected Products and Solution.

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 3WA COM190 is an accessory module for 3WA circuit breakers and provides connectivity via PROFINET IO and Modbus TCP.

SENTRON 3WL COM35 is an accessory module for 3WL circuit breakers and provides connectivity via PROFINET IO and Modbus TCP.

SENTRON 7KM PAC Switched Ethernet PROFINET Expansion Module is a plug-in device that provides switched Ethernet PROFINET V3 connectivity for 7KM PAC32x0 / 4200 and 3VA COM100/800 devices.

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-2020-35683

The code that parses ICMP packets relies on an unchecked value of the IP payload size (extracted from the IP header) to compute the ICMP checksum. When the IP payload size is set to be smaller than the size of the IP header, the ICMP checksum computation function may read out of bounds.

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:H/A:N/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2020-35684

The code that parses TCP packets relies on an unchecked value of the IP payload size (extracted from the IP header) to compute the length of the TCP payload within the TCP checksum computation function. When the IP payload size is set to be smaller than the size of the IP header, the TCP checksum computation function may read out of bounds. A low-impact write-out-of-bounds is also possible.

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-20: Improper Input Validation

Vulnerability CVE-2020-35685

TCP ISNs are generated in a predictable manner.

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:H/A:N/E:P/RL:O/RC:C
CWE	CWE-330: Use of Insufficiently Random Values

Vulnerability CVE-2021-31401

The TCP header processing code doesn't sanitize the length of the IP length (header + data). With a crafted IP packet an integer overflow would occur whenever the length of the IP data is calculated by subtracting the length of the header from the length of the total IP packet.

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:H/A:N/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Bundesamt für Sicherheit in der Informationstechnik (BSI) for coordination efforts
- CERT Coordination Center (CERT/CC) for coordination efforts
- Daniel dos Santos, Jos Wetzels, and Amine Amri from Forescout Technologies for coordinated disclosure
- Asaf Karas and Shachar Menashe from Vdoo for coordinated disclosure
- HCC Embedded for coordination efforts

ADDITIONAL INFORMATION

The products listed in this advisory are only affected by the subset of vulnerabilities listed here. They are not affected by the other vulnerabilities that are part of the “INFRA:HALT” publication.

For more details regarding the vulnerabilities in Interniche IP stack refer to:

- HCC Embedded security advisories: https://www.hcc-embedded.com/support/security-advisories
- Forescout publication “INFRA:HALT”: https://www.forescout.com/blog/new-critical-operational-technology-vulnerabilities-found-on-nichestack/

- CERT/CC Advisory VU#608209: https://kb.cert.org/vuls/id/608209

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 (2021-08-04):	Publication Date
V1.1 (2021-09-14):	Split SENTRON 7KM PAC Switched Ethernet PROFINET Expansion Module into three products (MLFBs); updated link to solution for SENTRON 3WA COM190
V1.2 (2022-01-11):	Added solution for SENTRON 7KM PAC Switched Ethernet PROFINET Expansion Module (7KM9300-0AE01-0AA0)

TERMS OF USE