SSA-180579: Privilege Management Vulnerability and Multiple Nucleus RTOS Vulnerabilities in APOGEE/TALON Field Panels before V3.5.5/V2.8.20

Publication Date: 2022-12-13
Last Update: 2023-08-08
Current Version: V1.1
CVSS v3.1 Base Score: 8.8

SUMMARY

APOGEE PXC / TALON TC field panels (BACnet before V3.5.5 and P2 Ethernet before V2.8.20) contain multiple vulnerabilities:

- CVE-2022-45937: A privilege management vulnerability that could allow low privilege authenticated attackers to gain high privilege access.
- CVE-2020-28388: Predictable Initial Sequence Numbers in the TCP/IP Stack of Nucleus RTOS (real-time operating system) used by the affected products.
- Several vulnerabilities in the DNS (domain name service) implementation of Nucleus RTOS.

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
APOGEE PXC Compact (BACnet): All versions < V3.5.5	Update to V3.5.5 or later version https://partnerportal.extranet.dc.siemens.com/
APOGEE PXC Compact (P2 Ethernet): All versions < V2.8.20	Update to V2.8.20 or later version https://partnerportal.extranet.dc.siemens.com/
APOGEE PXC Modular (BACnet): All versions < V3.5.5	Update to V3.5.5 or later version https://partnerportal.extranet.dc.siemens.com/
APOGEE PXC Modular (P2 Ethernet): All versions < V2.8.20	Update to V2.8.20 or later version https://partnerportal.extranet.dc.siemens.com/
TALON TC Compact (BACnet): All versions < V3.5.5	Update to V3.5.5 or later version https://partnerportal.extranet.dc.siemens.com/
TALON TC Modular (BACnet): All versions < V3.5.5	Update to V3.5.5 or later version https://partnerportal.extranet.dc.siemens.com/

WORKAROUNDS AND MITIGATIONS

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure Siemens strongly recommends to protect network access to affected products with appropriate mechanisms. It is advised to follow recommended security practices in order to run the devices in a protected IT environment.

PRODUCT DESCRIPTION

APOGEE PXC Modular and Compact Series devices are high-performance Direct Digital Control (DDC) devices and an integral part of the APOGEE Automation System.

TALON TC Modular and Compact Series devices are high-performance Direct Digital Control (DDC) devices and an integral part of the TALON Automation System.

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-2020-15795

The DNS domain name label parsing functionality does not properly validate the names in DNS-responses. The parsing of malformed responses could result in a write past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to execute code in the context of the current process or cause a denial-of-service condition.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2020-27009

The DNS domain name record decompression functionality does not properly validate the pointer offset values. The parsing of malformed responses could result in a write past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to execute code in the context of the current process or cause a denial-of-service condition.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-823: Use of Out-of-range Pointer Offset

Vulnerability CVE-2020-27736

The DNS domain name label parsing functionality does not properly validate the null-terminated name in DNS-responses. The parsing of malformed responses could result in a read past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to cause a denial-of-service condition or leak the read memory.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-170: Improper Null Termination

Vulnerability CVE-2020-27737

The DNS response parsing functionality does not properly validate various length and counts of the records. The parsing of malformed responses could result in a read past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to cause a denial-of-service condition or leak the memory past the allocated structure.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2020-27738

The DNS domain name record decompression functionality does not properly validate the pointer offset values. The parsing of malformed responses could result in a read access past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to cause a denial-of-service condition.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-788: Access of Memory Location After End of Buffer

Vulnerability CVE-2020-28388

Initial Sequence Numbers (ISNs) for TCP connections are derived from an insufficiently random source. As a result, the ISN of current and future TCP connections could be predictable. An attacker could hijack existing sessions or spoof future ones.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-342: Predictable Exact Value from Previous Values

Vulnerability CVE-2021-25677

The DNS client does not properly randomize DNS transaction IDs. That could allow an attacker to poison the DNS cache or spoof DNS resolving.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-330: Use of Insufficiently Random Values

Vulnerability CVE-2022-45937

A low privilege authenticated attacker with network access to the integrated web server could download sensitive information from the device containing user account credentials.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Abhishek Ramchandran for reporting the vulnerability CVE-2022-45937

ADDITIONAL INFORMATION

Products listed in this advisory use the Nucleus RTOS (Real-time operating system).

For more details regarding the vulnerabilities reported for Nucleus RTOS refer to Siemens Security Advisories:

- https://cert-portal.siemens.com/productcert/html/ssa-185699.html (CVE-2020-15795, CVE-2020-27009)
- https://cert-portal.siemens.com/productcert/html/ssa-705111.html (CVE-2020-27736, CVE-2020-27737, CVE-2020-27738, CVE-2021-25677)
- https://cert-portal.siemens.com/productcert/html/ssa-362164.html (CVE-2020-28388)

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 (2022-12-13):	Publication Date
V1.1 (2023-08-08):	Added additional vulnerabilities that were fixed in the same product versions (V3.5.5 / V2.8.20)

TERMS OF USE