

SSA-944498: Buffer Overflow Vulnerability in Web Server of APOGEE and TALON Automation Devices

Publication Date: 2021-09-14
Last Update: 2021-09-14
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

A buffer overflow vulnerability in the integrated web server of multiple APOGEE and TALON automation devices could allow a remote attacker to execute arbitrary code on the devices with root privileges.

Affected devices include the APOGEE MBC/MEC/PXC P2 Ethernet devices with Power Open Processors (PPC), APOGEE PXC BACnet devices, and TALON TC BACnet devices.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
APOGEE MBC (PPC) (P2 Ethernet): All versions >= V2.6.3	See recommendations from section Workarounds and Mitigations
APOGEE MEC (PPC) (P2 Ethernet): All versions >= V2.6.3	See recommendations from section Workarounds and Mitigations
APOGEE PXC Compact (BACnet): All versions < V3.5.3	Update to V3.5.3 or later version https://partnerportal.extranet.dc.siemens.com/ (login required)
APOGEE PXC Compact (P2 Ethernet): All versions >= V2.8	See recommendations from section Workarounds and Mitigations
APOGEE PXC Modular (BACnet): All versions < V3.5.3	Update to V3.5.3 or later version https://partnerportal.extranet.dc.siemens.com/ (login required)
APOGEE PXC Modular (P2 Ethernet): All versions >= V2.8	See recommendations from section Workarounds and Mitigations
TALON TC Compact (BACnet): All versions < V3.5.3	Update to V3.5.3 or later version https://partnerportal.extranet.dc.siemens.com/ (login required)
TALON TC Modular (BACnet): All versions < V3.5.3	Update to V3.5.3 or later version https://partnerportal.extranet.dc.siemens.com/ (login required)

WORKAROUNDS AND MITIGATIONS

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

- Please contact your local Siemens office for support
- Restrict access to the device, especially to the web interface (80/tcp and 443/tcp), to trusted IP addresses only
- Disable the integrated web server

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

The APOGEE MEC and the MBC are high-performance Direct Digital Control (DDC) devices and are an integral part of the APOGEE Automation System.

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

The TALON TC Modular and Compact Series 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-2021-27391

The web server of affected devices lacks proper bounds checking when parsing the Host parameter in HTTP requests, which could lead to a buffer overflow.

An unauthenticated remote attacker could exploit this vulnerability to execute arbitrary code on the device with root privileges.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:T/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Paul Noalhyt and David Doggett from Red Balloon Security for coordinated disclosure

ADDITIONAL INFORMATION

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 (2021-09-14): Publication Date

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.