# SSA-436469: TCP Vulnerability in APOGEE/TALON Field Panels

Publication Date: 2022-12-13
Last Update: 2022-12-13
Current Version: V1.0
CVSS v3.1 Base Score: 6.5

## SUMMARY

A TCP sequence vulnerability in the APOGEE PXC and TALON TC series of products could allow an attacker to execute a denial of service attack by sending specially crafted packets to the device.

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

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-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 |

## 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 (2022-12-13): 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.