# SSA-824231: Unauthenticated Firmware Upload Vulnerability in Desigo PX Controllers

Publication Date: 2018-01-24
Last Update: 2023-06-13
Current Version: V1.4
CVSS v3.1 Base Score: 9.8

## SUMMARY

Several Desigo PXC/PXM devices contain a vulnerability that could allow unauthenticated remote attackers to upload malicious firmware without prior authentication.

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 |
|---|---|
| Desigo PXC00-E.D V4.10:<br>All versions < V4.10.111 | Update to V4.10.111 or later version |
| Desigo PXC00-E.D V5.00:<br>All versions < V5.0.171 | Update to V5.0.171 or later version |
| Desigo PXC00-E.D V5.10:<br>All versions < V5.10.69 | Update to V5.10.69 or later version |
| Desigo PXC00-E.D V6.00:<br>All versions < V6.0.204 | Update to V6.0.204 or later version |
| Desigo PXC00/64/128-U V4.10:<br>All versions < V4.10.111 only with web module | Update to V4.10.111 or later version |
| Desigo PXC00/64/128-U V5.00:<br>All versions < V5.0.171 only with web module | Update to V5.0.171 or later version |
| Desigo PXC00/64/128-U V5.10:<br>All versions < V5.10.69 only with web module | Update to V5.10.69 or later version |
| Desigo PXC00/64/128-U V6.00:<br>All versions < V6.0.204 only with web module | Update to V6.0.204 or later version |
| Desigo PXC001-E.D V4.10:<br>All versions < V4.10.111 | Update to V4.10.111 or later version |
| Desigo PXC001-E.D V5.00:<br>All versions < V5.0.171 | Update to V5.0.171 or later version |
| Desigo PXC001-E.D V5.10:<br>All versions < V5.10.69 | Update to V5.10.69 or later version |
| Desigo PXC001-E.D V6.00:<br>All versions < V6.0.204 | Update to V6.0.204 or later version |

| | |
|---|---|
| Desigo PXC12-E.D V4.10:<br>All versions < V4.10.111 | Update to V4.10.111 or later version |
| Desigo PXC12-E.D V5.00:<br>All versions < V5.0.171 | Update to V5.0.171 or later version |
| Desigo PXC12-E.D V5.10:<br>All versions < V5.10.69 | Update to V5.10.69 or later version |
| Desigo PXC12-E.D V6.00:<br>All versions < V6.0.204 | Update to V6.0.204 or later version |
| Desigo PXC22-E.D V4.10:<br>All versions < V4.10.111 | Update to V4.10.111 or later version |
| Desigo PXC22-E.D V5.00:<br>All versions < V5.0.171 | Update to V5.0.171 or later version |
| Desigo PXC22-E.D V5.10:<br>All versions < V5.10.69 | Update to V5.10.69 or later version |
| Desigo PXC22-E.D V6.00:<br>All versions < V6.0.204 | Update to V6.0.204 or later version |
| Desigo PXC22.1-E.D V4.10:<br>All versions < V4.10.111 | Update to V4.10.111 or later version |
| Desigo PXC22.1-E.D V5.00:<br>All versions < V5.0.171 | Update to V5.0.171 or later version |
| Desigo PXC22.1-E.D V5.10:<br>All versions < V5.10.69 | Update to V5.10.69 or later version |
| Desigo PXC22.1-E.D V6.00:<br>All versions < V6.0.204 | Update to V6.0.204 or later version |
| Desigo PXC36.1-E.D V4.10:<br>All versions < V4.10.111 | Update to V4.10.111 or later version |
| Desigo PXC36.1-E.D V5.00:<br>All versions < V5.0.171 | Update to V5.0.171 or later version |
| Desigo PXC36.1-E.D V5.10:<br>All versions < V5.10.69 | Update to V5.10.69 or later version |
| Desigo PXC36.1-E.D V6.00:<br>All versions < V6.0.204 | Update to V6.0.204 or later version |
| Desigo PXC50-E.D V4.10:<br>All versions < V4.10.111 | Update to V4.10.111 or later version |
| Desigo PXC50-E.D V5.00:<br>All versions < V5.0.171 | Update to V5.0.171 or later version |

| | |
|---|---|
| Desigo PXC50-E.D V5.10:<br>All versions < V5.10.69 | Update to V5.10.69 or later version |
| Desigo PXC50-E.D V6.00:<br>All versions < V6.0.204 | Update to V6.0.204 or later version |
| Desigo PXC100-E.D V4.10:<br>All versions < V4.10.111 | Update to V4.10.111 or later version |
| Desigo PXC100-E.D V5.00:<br>All versions < V5.0.171 | Update to V5.0.171 or later version |
| Desigo PXC100-E.D V5.10:<br>All versions < V5.10.69 | Update to V5.10.69 or later version |
| Desigo PXC100-E.D V6.00:<br>All versions < V6.0.204 | Update to V6.0.204 or later version |
| Desigo PXC200-E.D V4.10:<br>All versions < V4.10.111 | Update to V4.10.111 or later version |
| Desigo PXC200-E.D V5.00:<br>All versions < V5.0.171 | Update to V5.0.171 or later version |
| Desigo PXC200-E.D V5.10:<br>All versions < V5.10.69 | Update to V5.10.69 or later version |
| Desigo PXC200-E.D V6.00:<br>All versions < V6.0.204 | Update to V6.0.204 or later version |
| Desigo PXM20-E V4.10:<br>All versions < V4.10.111 | Update to V4.10.111 or later version |
| Desigo PXM20-E V5.00:<br>All versions < V5.0.171 | Update to V5.0.171 or later version |
| Desigo PXM20-E V5.10:<br>All versions < V5.10.69 | Update to V5.10.69 or later version |
| Desigo PXM20-E V6.00:<br>All versions < V6.0.204 | Update to V6.0.204 or later version |

## 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

Desigo PXC00/64/128-U are automation stations with P-bus and PPS2 connections.

Desigo PXC00-E.D: System controller BACnet/IP. Article No: BPZ:PXC00-E.D

Desigo PXC001-E.D: System controller for the integration of KNX, M-Bus, Modbus or SCL over BACnet/IP. Article No: S55372-C114

Desigo PXC100-E.D: Automation station BACnet/IP, with up to 200 data points. Article No: BPZ:PXC100-E.D

Desigo PXC12-E.D: Automation station with 12 data points and BACnet on IP. Article No: BPZ:PXC12-E.D

Desigo PXC200-E.D: Automation station BACnet/IP, with more than 200 data points. Article No: BPZ:PXC200-E.D

Desigo PXC22-E.D: Automation station with 22 data points and BACnet on IP. Article No: BPZ:PXC22-E.D

Desigo PXC22.1-E.D: Automation station with 22 data points, extendable and BACnet on IP. Article No: S55372-C119

Desigo PXC36.1-E.D: Automation station with 36 data points, extendable and BACnet on IP. Article No: S55372-C121

Desigo PXC50-E.D: Automation station BACnet/IP, with up to 80 data points. Article No: S55372-C110

Desigo PXM20-E: Operator unit with BACnet on IP. Article No: BPZ:PXM20-E

## 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-2018-4834

A remote attacker with network access to the device could potentially upload a new firmware image to the devices without prior authentication.

| | |
|---|---|
| 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:O/RC:C |
| CWE | CWE-306: Missing Authentication for Critical Function |

## ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Can Demirel and Melih Berk Ekşioğlu from Biznet Bilişim for coordinated disclosure
- Industrial Control System Cyber Emergency Response Team (ICS-CERT) for coordination efforts

## ADDITIONAL INFORMATION

Firmware versions for the affected products can be obtained from Siemens customer support or a local partner.

This advisory covers only the Desigo PX Controller product line and not the Apogee PX Controller product line.

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 (2018-01-24): | Publication Date |
| V1.1 (2018-02-05): | Removed broken links |
| V1.2 (2018-03-20): | Clarified that Apogee PX product line is out of scope |
| V1.3 (2019-03-12): | Older firmware versions added |
| V1.4 (2023-06-13): | Listed the affected product version lines and associated fix versions explicitly; no significant change of contents compared to previous advisory release (2019-03-12) |

## TERMS OF USE