SSA-824231: Unauthenticated Firmware Upload Vulnerability in Desigo PXC

Publication Date: 2018-01-24
Last Update: 2018-01-24
Current Version: V1.0
CVSS v3.0 Base Score: 9.8

SUMMARY

The latest update for Desigo PXC devices fixes a vulnerability that could allow unauthenticated remote attackers to upload malicious firmware without prior authentication.
Siemens recommends updating to the new version.

AFFECTED PRODUCTS AND SOLUTION

<table>
<thead>
<tr>
<th>Affected Product and Versions</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desigo Automation Controllers Compact PXC12/22/36-E.D: All versions &lt; V6.00.204</td>
<td>Install V6.00.204 or a later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109481602">https://support.industry.siemens.com/cs/ww/en/view/109481602</a></td>
</tr>
<tr>
<td>Desigo Automation Controllers Modular PXC00/50/100/200-E.D: All versions &lt; V6.00.204</td>
<td>Install V6.00.204 or a later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109481602">https://support.industry.siemens.com/cs/ww/en/view/109481602</a></td>
</tr>
<tr>
<td>Desigo Automation Controllers PXC00/64/128-U with Web module: All versions &lt; V6.00.204</td>
<td>Install V6.00.204 or a later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109481602">https://support.industry.siemens.com/cs/ww/en/view/109481602</a></td>
</tr>
<tr>
<td>Desigo Automation Controllers for Integration PXC001-E.D: All versions &lt; V6.00.204</td>
<td>Install V6.00.204 or a later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109481602">https://support.industry.siemens.com/cs/ww/en/view/109481602</a></td>
</tr>
<tr>
<td>Desigo Operator Unit PXM20-E: All versions &lt; V6.00.204</td>
<td>Install V6.00.204 or a later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109481602">https://support.industry.siemens.com/cs/ww/en/view/109481602</a></td>
</tr>
</tbody>
</table>

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any specific mitigations or workarounds.

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 Desigo PX automation stations and operator units control and monitor building automation systems. They allow for alarm signaling, time-based programs and trend logging.

**VULNERABILITY CLASSIFICATION**

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

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.

<table>
<thead>
<tr>
<th>CVSS v3.0 Base Score</th>
<th>9.8</th>
</tr>
</thead>
</table>

**ACKNOWLEDGMENTS**

Siemens thanks the following parties for their efforts:

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

**ADDITIONAL INFORMATION**

For further inquiries on 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

**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.