SSA-360783: Multiple Webserver Vulnerabilities in Desigo PXM Devices

Publication Date: 2022-10-11
Last Update: 2022-10-11
Current Version: V1.0
CVSS v3.1 Base Score: 8.8

SUMMARY

Desigo PXM devices contain multiple vulnerabilities in the webserver application that could allow an attacker to potentially access sensitive information, execute arbitrary commands, cause a denial of service condition, or perform remote code execution.

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 PXM30-1: All versions < V02.20.126.11-41	Update to V02.20.126.11-41 or later version. Please contact your local Siemens office for additional support in obtaining the update. https://support.industry.siemens.com/cs/ww/en/view/109813821
Desigo PXM30.E: All versions < V02.20.126.11-41	Update to V02.20.126.11-41 or later version. Please contact your local Siemens office for additional support in obtaining the update. https://support.industry.siemens.com/cs/ww/en/view/109813821
Desigo PXM40-1: All versions < V02.20.126.11-41	Update to V02.20.126.11-41 or later version. Please contact your local Siemens office for additional support in obtaining the update. https://support.industry.siemens.com/cs/ww/en/view/109813821
Desigo PXM40.E: All versions < V02.20.126.11-41	Update to V02.20.126.11-41 or later version. Please contact your local Siemens office for additional support in obtaining the update. https://support.industry.siemens.com/cs/ww/en/view/109813821
Desigo PXM50-1: All versions < V02.20.126.11-41	Update to V02.20.126.11-41 or later version. Please contact your local Siemens office for additional support in obtaining the update. https://support.industry.siemens.com/cs/ww/en/view/109813821

Desigo PXM50.E: All versions < V02.20.126.11-41	Update to V02.20.126.11-41 or later version. Please contact your local Siemens office for additional support in obtaining the update. https://support.industry.siemens.com/cs/ww/en/view/109813821
PXG3.W100-1: All versions < V02.20.126.11-37	Update to V02.20.126.11-37 or later version. Please contact your local Siemens office for additional support in obtaining the update. https://support.industry.siemens.com/cs/ww/en/view/109813821
PXG3.W100-2: All versions < V02.20.126.11-41	Update to V02.20.126.11-41 or later version. Please contact your local Siemens office for additional support in obtaining the update. https://support.industry.siemens.com/cs/ww/en/view/109813821
PXG3.W200-1: All versions < V02.20.126.11-37	Update to V02.20.126.11-37 or later version. Please contact your local Siemens office for additional support in obtaining the update. https://support.industry.siemens.com/cs/ww/en/view/109813821
PXG3.W200-2: All versions < V02.20.126.11-41	Update to V02.20.126.11-41 or later version. Please contact your local Siemens office for additional support in obtaining the update. https://support.industry.siemens.com/cs/ww/en/view/109813821

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 PXG3.Wx00-y - Desigo BACnet/IP Web Interface with standard or extended functionality These devices have a web server that processes data from various Desigo automation stations and other devices based on BACnet IP to HTML5 web pages. They are used as an interface for web-based, graphical operation of BACnet automation stations using Desigo touch panels and devices with an HTML 5.0 web browser. The web interfaces PXG3.W100-1/2 and PXG3.W200-1/2 are the central points of access to operate the automation level and room automation.

Desigo PXMxx-1 - Desigo Control Point with embedded web browser. These high quality touch panels are used for technical on-site operation of plants as well as room operation. They are optimized for local on-site operation of the Desigo building automation and control system. These touch panels have an

embedded web browser that is used for communicating with HTML5.0 capable web servers and utilizes TCP/IP communication.

Desigo PXMxx.E - Desigo Control Point with integrated web server. These high quality touch panels are used for technical on-site operation of plants as well as room operation. They are optimized for local on-site operation of the Desigo building automation and control system. These touch panels have an integrated web server and utilizes BACnet/IP communication.

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-2022-40176

There exists an Improper Neutralization of Special Elements used in an OS Command with root privileges during a restore operation due to the missing validation of the names of files included in the input package. By restoring a specifically crafted package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise.

CVSS v3.1 Base Score	8.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Vulnerability CVE-2022-40177

Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon queries, a remote low-privileged attacker can read sensitive files on the device.

CVSS v3.1 Base Score	5.7
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2022-40178

Improper Neutralization of Input During Web Page Generation exists in the "Import Files" functionality of the "Operation" web application, due to the missing validation of the titles of files included in the input package. By uploading a specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code.

CVSS v3.1 Base Score	4.8
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2022-40179

A Cross-Site Request Forgery exists in endpoints of the “Operation” web application that interpret and execute Axon language queries, due to the missing validation of anti-CSRF tokens or other origin checks. By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated attacker can execute arbitrary Axon queries against the device.

CVSS v3.1 Base Score	6.8
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-352: Cross-Site Request Forgery (CSRF)

Vulnerability CVE-2022-40180

A Cross-Site Request Forgery exists in the “Import Files“ functionality of the “Operation” web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote unauthenticated attacker can upload and enable permanent arbitrary JavaScript code into the device just by convincing a victim to visit a specifically crafted webpage while logged-in to the device web application.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-352: Cross-Site Request Forgery (CSRF)

Vulnerability CVE-2022-40181

The device embedded browser does not prevent interaction with alternative URI schemes when redirected to corresponding resources by web application code. By setting the homepage URI, the favorite URIs, or redirecting embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary JavaScript code in order to steal or manipulate the information on the screen, or trigger denial of service conditions.

CVSS v3.1 Base Score	8.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H/E:P/RL:O/RC:C
CWE	CWE-84: Improper Neutralization of Encoded URI Schemes in a Web Page

Vulnerability CVE-2022-40182

The device embedded Chromium-based browser is launched as root with the “–no-sandbox” option. Attackers can add arbitrary JavaScript code inside “Operation” graphics and successfully exploit any number of publicly known vulnerabilities against the version of the embedded Chromium-based browser.

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-250: Execution with Unnecessary Privileges

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Andrea Palanca from Nozomi Networks 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 (2022-10-11): Publication Date

TERMS OF USE