SSA-626968: Multiple Webserver Vulnerabilities in Desigo PXC and DXR Devices

Publication Date: 2022-05-10
Last Update: 2022-06-14
Current Version: V1.1
CVSS v3.1 Base Score: 9.0

SUMMARY

Desigo PXC3, PXC4, PXC5 and DXR2 devices contain multiple vulnerabilities in the webserver application that could allow an attacker to potentially intercept unencrypted transmission of sensitive information, 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 DXR2: All versions < V01.21.142.5-22 only affected by CVE-2022-24040, CVE-2022-24041, CVE-2022-24042, CVE-2022-24043, CVE-2022-24044, CVE-2022-24045	Update to V01.21.142.5-22 or later version. Please contact your local Siemens office for additional support in obtaining the update.
Desigo PXC3: All versions < V01.21.142.4-18 only affected by CVE-2022-24040, CVE-2022-24041, CVE-2022-24042, CVE-2022-24043, CVE-2022-24044, CVE-2022-24045	Update to V01.21.142.4-18 or later version. Please contact your local Siemens office for additional support in obtaining the update.
Desigo PXC4: All versions < V02.20.142.10-10884	Update to V02.20.142.10-10884 or later version. Please contact your local Siemens office for additional support in obtaining the update.
Desigo PXC5: All versions < V02.20.142.10-10884	Update to V02.20.142.10-10884 or later version. Please contact your local Siemens office for additional support in obtaining the update.

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 Desigo DXR2 controllers are compact, programmable automation stations with increased functionality and flexibility to support the demands for standard control of terminal HVAC equipment and TRA (Total Room Automation) applications.

The Desigo PXC3 series room automation stations can be used for buildings with more sophisticated requirements on functionality and flexibility. Desigo Room Automation is used when several disciplines (HVAC, lighting, shading) are combined to form one solution and when high flexibility is required.

The Desigo PXC4 building automation controller was designed for HVAC systems controls. It was developed as a compact device with built in IOs with the ability to expand to your needs using addition TX-IO modules.

The Desigo PXC5 is a freely programmable controller for BACnet system-level functions such as alarm routing, system-wide scheduling and trending, as well as device monitoring.

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-2022-24039

The "addCell" JavaScript function fails to properly sanitize user-controllable input before including it into the generated XML body of the XLS report document, such that it is possible to inject arbitrary content (e.g., XML tags) into the generated file.

An attacker with restricted privileges, by poisoning any of the content used to generate XLS reports, could be able to leverage the application to deliver malicious files against higher-privileged users and obtain Remote Code Execution (RCE) against the administrator's workstation.

CVSS v3.1 Base Score	9.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-75: Failure to Sanitize Special Elements into a Different Plane (Special Element Injection)

Vulnerability CVE-2022-24040

The web application fails to enforce an upper bound to the cost factor of the PBKDF2 derived key during the creation or update of an account.

An attacker with the user profile access privilege could cause a denial of service (DoS) condition through CPU consumption by setting a PBKDF2 derived key with a remarkably high cost effort and then attempting a login to the so-modified account.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

Vulnerability CVE-2022-24041

The web application stores the PBKDF2 derived key of users passwords with a low iteration count.

An attacker with user profile access privilege can retrieve the stored password hashes of other accounts and then successfully perform an offline cracking attack and recover the plaintext passwords of other users.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-916: Use of Password Hash With Insufficient Computational Effort

Vulnerability CVE-2022-24042

The web application returns an AuthToken that does not expire at the defined auto logoff delay timeout.

An attacker could be able to capture this token and re-use old session credentials or session IDs for authorization.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-613: Insufficient Session Expiration

Vulnerability CVE-2022-24043

The login functionality of the application fails to normalize the response times of login attempts performed with wrong usernames with the ones executed with correct usernames.

A remote unauthenticated attacker could exploit this side-channel information to perform a username enumeration attack and identify valid usernames.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-203: Observable Discrepancy

Vulnerability CVE-2022-24044

The login functionality of the application does not employ any countermeasures against Password Spraying attacks or Credential Stuffing attacks.

An attacker could obtain a list of valid usernames on the device by exploiting the issue and then perform a precise Password Spraying or Credential Stuffing attack in order to obtain access to at least one account.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-307: Improper Restriction of Excessive Authentication Attempts

Vulnerability CVE-2022-24045

The application, after a successful login, sets the session cookie on the browser via client-side JavaScript code, without applying any security attributes (such as “Secure”, “HttpOnly”, or “SameSite”).

Any attempts to browse the application via unencrypted HTTP protocol would lead to the transmission of all his/her session cookies in plaintext through the network. An attacker could then be able to sniff the network and capture sensitive information.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-614: Sensitive Cookie in HTTPS Session Without ‘Secure’ Attribute

ACKNOWLEDGMENTS

Siemens thanks the following parties for their 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 (2022-05-10): Publication Date
V1.1 (2022-06-14): Added steps to contact local Siemens office for obtaining update

TERMS OF USE