

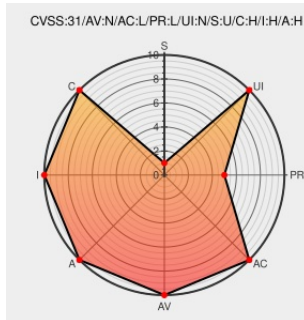


CVE-2022-40182

Published on: Not Yet Published

Last Modified on: 10/12/2022 03:45:00 PM UTC

CVE-2022-40182

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Designo Pxm30-1](#) from [Siemens](#) contain the following vulnerability:

A vulnerability has been identified in Designo PXM30-1 (All versions < V02.20.126.11-41), Designo PXM30.E (All versions < V02.20.126.11-41), Designo PXM40-1 (All versions < V02.20.126.11-41), Designo PXM40.E (All versions < V02.20.126.11-41), Designo PXM50-1 (All versions < V02.20.126.11-41), Designo PXM50.E (All versions <

V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). 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.

CVE-2022-40182 has been assigned by [S](#) productcert@siemens.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
	cert-portal.siemens.com application/pdf	MISC cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further,

Related QID Numbers

[591423](#) Siemens Desigo Control Point Devices (PXM and PXG3) Webserver Multiple Security Vulnerabilities (SSA-360783)

Exploit/POC from Github

A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Siemens	Desigo Pxm30-1	-	All	All	All
Operating System	Siemens	Desigo Pxm30-1 Firmware	All	All	All	All
Hardware 	Siemens	Desigo Pxm30.e	-	All	All	All
Operating System	Siemens	Desigo Pxm30.e Firmware	All	All	All	All
Hardware 	Siemens	Desigo Pxm40-1	-	All	All	All
Operating System	Siemens	Desigo Pxm40-1 Firmware	All	All	All	All
Hardware 	Siemens	Desigo Pxm40.e	-	All	All	All
Operating System	Siemens	Desigo Pxm40.e Firmware	All	All	All	All
Hardware 	Siemens	Desigo Pxm50-1	-	All	All	All
Operating System	Siemens	Desigo Pxm50-1 Firmware	All	All	All	All
Hardware 	Siemens	Desigo Pxm50.e	-	All	All	All
Operating System	Siemens	Desigo Pxm50.e Firmware	All	All	All	All
Hardware 	Siemens	Pxm3.w100-1	-	All	All	All
Operating System	Siemens	Pxm3.w100-1 Firmware	All	All	All	All
Hardware 	Siemens	Pxm3.w100-2	-	All	All	All
Operating System	Siemens	Pxm3.w100-2 Firmware	All	All	All	All
Hardware 	Siemens	Pxm3.w200-1	-	All	All	All
Operating System	Siemens	Pxm3.w200-1 Firmware	All	All	All	All

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-40182 : A vulnerability has been identified in Desigo PXM30-1 All versions < V02.20.126.11-41 , Desigo PX... twitter.com/i/web/status/1...	2022-10-11 10:28:30
 /r/netcve	CVE-2022-40182	2022-10-11 10:38:33

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)