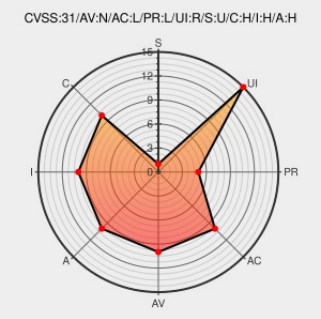
CVE-2022-40176

Published on: Not Yet Published

Last Modified on: 10/12/2022 04:45:00 PM UTC

CVE-2022-40176

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Desigo Pxm30-1 from Siemens contain the following vulnerability:

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

CVE-2022-40176 has been assigned by productcert@siemens.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
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, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

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

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	Pxg3.w100-1	-	All	All	All
Operating System	Siemens	Pxg3.w100-1 Firmware	All	All	All	All
Hardware	Siemens	Pxg3.w100-2	-	All	All	All
Operating System	Siemens	Pxg3.w100-2 Firmware	All	All	All	All
Hardware	Siemens	Pxg3.w200-1	-	All	All	All
Operating System	Siemens	Pxg3.w200-1 Firmware	All	All	All	All
Hardware	Siemens	Pxg3.w200-2	-	All	All	All
Operating System	Siemens	Pxg3.w200-2 Firmware	All	All	All	All

cpe:2.3:h:siemens:desigo_pxm30-1:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:desigo_pxm30-1_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:desigo_pxm30.e:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:desigo_pxm30.e_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:desigo_pxm40-1:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:desigo_pxm40-1_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:desigo_pxm40.e:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:desigo_pxm40.e_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:desigo_pxm50-1:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:desigo_pxm50-1_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:desigo_pxm50.e:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:desigo_pxm50.e_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:pxg3.w100-1:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:pxg3.w100-1_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:pxg3.w100-2:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:pxg3.w100-2_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:pxg3.w200-1:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:pxg3.w200-1_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:pxg3.w200-2:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:pxg3.w200-2_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-40176 : 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 10:26:26
/r/netcve	CVE-2022-40176	2022-10-11 10:38:28

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report