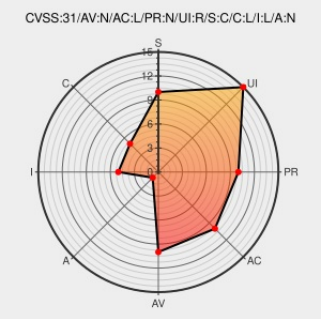
CVE-2023-4296

Published on: Not Yet Published

Last Modified on: 09/18/2023 04:15:00 PM UTC

CVE-2023-4296

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



Certain versions of Codebeamer from Intland contain the following vulnerability:

If an attacker tricks an admin user of PTC Codebeamer into clicking on a malicious link, it may allow the attacker to inject arbitrary code to be executed in the browser on the target device.

CVE-2023-4296 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **PTC** - **Codebeamer** version **not down converted**

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
PTC Codebeamer | CISA	www.cisa.gov text/html	MISC www.cisa.gov/news-events/ics-advisories/icsa-23-241-01
PTC - Codebeamer Cross Site Scripting ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/174703/PTC-Codebeamer-Cross-Site-Scripting.html
Security Vulnerabilities Identified in Codebeamer - CVE-2023-4296	codebeamer.com text/html	MISC codebeamer.com/cb/wiki/31346480
Full Disclosure: SEC Consult SA-20230829-0 :: Reflected Cross-Site Scripting (XSS) in PTC - Codebeamer (ALM Solution)	seclists.org text/html	MISC seclists.org/fulldisclosure/2023/Sep/10

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Intland	Codebeamer	21.09.0	-	All	All
Application	Intland	Codebeamer	21.09.0	sp1	All	All
Application	Intland	Codebeamer	21.09.0	sp10	All	All
Application	Intland	Codebeamer	21.09.0	sp11	All	All
Application	Intland	Codebeamer	21.09.0	sp12	All	All
Application	Intland	Codebeamer	21.09.0	sp13	All	All
Application	Intland	Codebeamer	21.09.0	sp2	All	All
Application	Intland	Codebeamer	21.09.0	sp3	All	All
Application	Intland	Codebeamer	21.09.0	sp4	All	All
Application	Intland	Codebeamer	21.09.0	sp5	All	All
Application	Intland	Codebeamer	21.09.0	sp6	All	All
Application	Intland	Codebeamer	21.09.0	sp7	All	All
Application	Intland	Codebeamer	21.09.0	sp8	All	All
Application	Intland	Codebeamer	21.09.0	sp9	All	All
Application	Intland	Codebeamer	22.04.0	-	All	All
Application	Intland	Codebeamer	22.04.0	sp1	All	All
Application	Intland	Codebeamer	22.04.0	sp2	All	All
Application	Intland	Codebeamer	22.04.0	sp3	All	All
Application	Intland	Codebeamer	22.04.0	sp4	All	All
Application	Intland	Codebeamer	22.04.0	sp5	All	All
Application	Intland	Codebeamer	22.10.0	-	All	All
Application	Intland	Codebeamer	22.10.0	sp1	All	All
Application	Intland	Codebeamer	22.10.0	sp2	All	All
Application	Intland	Codebeamer	22.10.0	sp3	All	All
Application	Intland	Codebeamer	22.10.0	sp4	All	All
Application	Intland	Codebeamer	22.10.0	sp5	All	All
Application	Intland	Codebeamer	22.10.0	sp6	All	All
Application	Intland	Codebeamer	22.10.0	sp7	All	All
Application	Intland	Codebeamer	22.10.0	sp8	All	All

Application	intland	codebeamer	22.10.0	sp6	All	All

cpe:2.3:a:intland:codebeamer:21.09.0:-:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:21.09.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:21.09.0:sp10:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:21.09.0:sp11:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:21.09.0:sp12:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:21.09.0:sp13:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:21.09.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:21.09.0:sp3:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:21.09.0:sp4:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:21.09.0:sp5:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:21.09.0:sp6:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:21.09.0:sp7:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:21.09.0:sp8:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:21.09.0:sp9:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:22.04.0:-:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:22.04.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:22.04.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:22.04.0:sp3:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:22.04.0:sp4:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:22.04.0:sp5:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:22.10.0:-:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:22.10.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:22.10.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:22.10.0:sp3:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:22.10.0:sp4:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:22.10.0:sp5:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:22.10.0:sp6:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:22.10.0:sp7:*:*:*:*:*:*:

cpe:2.3:a:intland:codebeamer:22.10.0:sp8:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→