



CVE-2022-26111

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2022-26111
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-25 15:15:00 UTC
Updated	2023-08-08 14:21:00 UTC
Description	The BeanShell components of IRISNext through 9.8.28 allow execution of arbitrary commands on the target server by crea

Risk And Classification

Problem Types: CWE-917

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Canon	Irisnext	All	All	All	All

References

Reference	Source	Link	Tags
CVE-Advisory/CVE-2022-26111.pdf at main · post-cyberlabs/CVE-Advisory · GitHub	MISC	github.com	
IRISNEXT By I.R.I.S. group	MISC	varsnext.iriscorporate.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

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