



CVE-2023-43871

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-43871
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-28 14:15:00 UTC
Updated	2023-11-08 03:12:00 UTC
Description	A File upload vulnerability in WBCE v.1.6.1 allows a local attacker to upload a pdf file with hidden Cross Site Scripting (XSS)

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wbce	Wbce Cms	1.6.1	All	All	All

References

Reference
CVE-2023-43871-WBCE-Arbitrary-File-Upload--XSS---Media/README.md at main · sromanhu/CVE-2023-43871-WBCE-Arbitrary-File-Uploac
WBCE File Upload XSS - WBCE v1.6.1
CVE Program record
NVD vulnerability detail

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