



CVE-2022-32167

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

Summary

CVE	CVE-2022-32167
State	PUBLIC
Assigner	vulnerabilitylab@whitesourcesoftware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-20 15:15:00 UTC
Updated	2022-09-21 19:21:00 UTC
Description	Cloudeve versions v1.0.0 through v3.5.3 are vulnerable to Stored Cross-Site Scripting (XSS), via the file upload functional

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cloudeve	Cloudeve	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2022-32167 Mend Vulnerability Database	MISC	www.mend.io	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Daniel Elkabes

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

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](#)