



CVE-2022-27263

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

Summary

CVE	CVE-2022-27263
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-12 17:15:00 UTC
Updated	2022-04-19 19:28:00 UTC
Description	An arbitrary file upload vulnerability in the file upload module of Strapi v4.1.5 allows attackers to execute arbitrary code via :

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Strapi	Strapi	4.1.5	All	All	All

References

Reference	Source	Link	Tags
Strapi XSS Attack via File Name - YouTube	MISC	www.youtube.com	
GitHub - strapi/strapi: ????? Open source Node.js Headless CMS to easily build customisable APIs	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

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