



CVE-2023-39264

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

Summary

CVE	CVE-2023-39264
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-06 13:15:00 UTC
Updated	2023-09-11 14:28:00 UTC
Description	By default, stack traces for errors were enabled, which resulted in the exposure of internal traces on REST API endpoints tr

Risk And Classification

Problem Types: CWE-209

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Superset	All	All	All	All

References

Reference	Source	Link	Tags
lists.apache.org/thread/y65t1of7hb445n86o1vdzjct7rfwlx75	MISC	lists.apache.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[995303](#) Python (Pip) Security Update for apache-superset (GHSA-cpvx-2365-466c)

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