



CVE-2022-43566

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

Summary

CVE	CVE-2022-43566
State	PUBLIC
Assigner	prodsec@splunk.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-04 23:15:00 UTC
Updated	2023-11-07 03:53:00 UTC
Description	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, an authenticated user can run risky commands using a more p

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Splunk	Splunk	All	All	All	All
Application	Splunk	Splunk Cloud Platform	All	All	All	All

References

Reference	Source	Link	Tags
SVD-2022-1106 Splunk	MISC	www.splunk.com	
Splunk Data exfiltration from Analytics Workspace using sid query - Splunk Security Content	MISC	research.splunk.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.

Legacy QID Mappings

[378037](#) Splunk Enterprise Reflected Cross-Site Scripting (XSS) Vulnerability (SVD-2022-1108)

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

Free CVE JSON API cve.report/api

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