



CVE-2022-43570

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

Summary

CVE	CVE-2022-43570
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 8.1.12, 8.2.9, and 9.0.2, an authenticated user can perform an extensible markup language (XML) injection attack by sending a specially crafted request to the Splunk Enterprise web interface. This attack can be used to execute arbitrary code on the target system.

Risk And Classification

Problem Types: CWE-611

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-2022-1110 Splunk	MISC	www.splunk.com	
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

[378020](#) Splunk Enterprise Multiple Security Vulnerabilities (SVD-2022-1109, SVD-2022-1110)

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