CVE-2022-32156

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-32156
State	PUBLIC
Assigner	prodsec@splunk.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-15 17:15:00 UTC
Updated	2023-11-07 03:47:00 UTC
Description	In Splunk Enterprise and Universal Forwarder versions before 9.0, the Splunk command-line interface (CLI) did not validate

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Splunk	Splunk	All	All	All	All
Application	Splunk	Universal Forwarder	All	All	All	All

References

Reference	Source	Link	Tags
SVD-2022-0606 | Splunk	CONFIRM	www.splunk.com	
Configure TLS certificate host name validation - Splunk Documentation	CONFIRM	docs.splunk.com	
Security updates - Splunk Documentation	CONFIRM	docs.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

730544 Splunk Enterprise Improper Transport Layer Security (TLS) Certificate Validation (SVD-2022-0606)