CVE-2022-32153

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

Summary

CVE	CVE-2022-32153
State	PUBLIC
Assigner	prodsec@splunk.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-15 17:15:00 UTC
Updated	2022-06-24 01:22:00 UTC
Description	Splunk Enterprise peers in Splunk Enterprise versions before 9.0 and Splunk Cloud Platform versions before 8.2.2203 did r

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	Splunk Cloud Platform	All	All	All	All

References

Reference	Source	Link	Tags
Splunk Digital Certificates Lack of Encryption - Splunk Security Content	CONFIRM	research.splunk.com	
Splunk Digital Certificates Infrastructure Version - Splunk Security Content	CONFIRM	research.splunk.com	
Splunk protocol impersonation weak encryption selfsigned - Splunk Security Content	CONFIRM	research.splunk.com	
SVD-2022-0603 | 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	
Splunk Identified SSL TLS Certificates - Splunk Security Content	CONFIRM	research.splunk.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

Vendor Comments And Credit

Discovery Credit

LEGACY: Chris Green at Splunk

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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