



CVE-2021-3422

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

Summary

CVE	CVE-2021-3422
State	PUBLIC
Assigner	prodsec@splunk.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-25 19:15:00 UTC
Updated	2022-04-11 19:51:00 UTC
Description	The lack of validation of a key-value field in the Splunk-to-Splunk protocol results in a denial-of-service in Splunk Enterprise

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

References

Reference	Source	Link	Tags
Team82: Splunk Enterprise Indexer, Forwarder Vulnerability Patched	MISC	claroty.com	
SVD-2022-0301 Splunk	MISC	www.splunk.com	
Team82: Splunk Enterprise Indexer, Forwarder Vulnerability Patched	MISC	claroty.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Sharon Brizinov and Tal Keren of Claroty

Legacy QID Mappings

[730494](#) Splunk Enterprise Denial of Service (DoS) Vulnerability (SVD-2022-0301)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)