



CVE-2022-32158

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2022-32158
State	PUBLIC
Assigner	prodsec@splunk.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-15 17:15:00 UTC
Updated	2022-07-12 21:15:00 UTC
Description	Splunk Enterprise deployment servers in versions before 8.1.10.1, 8.2.6.1, and 9.0 let clients deploy forwarder bundles to o

Risk And Classification

Problem Types: NVD-CWE-noinfo

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
SVD-2022-0608 Splunk	CONFIRM	www.splunk.com	
Splunk Process Injection Forwarder Bundle Downloads - Splunk Security Content	MISC	research.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

Vendor Comments And Credit

Discovery Credit

LEGACY: Nadim Taha at Splunk

Legacy QID Mappings

730525 Splunk Enterprise Arbitrary Code Execution Vulnerability (SVD-2022-0608)

© [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](#)