

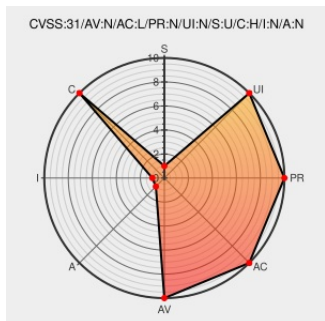


CVE-2022-32157

Published on: Not Yet Published

Last Modified on: 06/24/2022 12:51:00 AM UTC

CVE-2022-32157 - advisory for SVD-2022-0607

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Splunk](#) from [Splunk](#) contain the following vulnerability:

Splunk Enterprise deployment servers in versions before 9.0 allow unauthenticated downloading of forwarder bundles. Remediation requires you to update the deployment server to version 9.0 and Configure authentication for deployment servers and clients

(<https://docs.splunk.com/Documentation/Splunk/9.0.0/Security/ConfigDSDCAuthEnhancement>)
Once enabled, deployment servers can manage only Universal Forwarder versions 9.0 and higher. Though the vulnerability does not directly affect Universal Forwarders, remediation requires updating all Universal Forwarders that the deployment server manages to version 9.0 or higher prior to enabling the remediation.

CVE-2022-32157 has been assigned by [prodsec@splunk.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Splunk, Inc](#) - **Splunk Enterprise** version < 9.0

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

PARTIAL

NONE

NONE

CVE References

Description	Tags	Link
SVD-2022-0607 Splunk	www.splunk.com text/html	 CONFIRM www.splunk.com/en_us/product-security/announcements/svd-2022-0607.html
Splunk Process Injection Forwarder Bundle Downloads - Splunk Security Content	research.splunk.com text/html	 CONFIRM research.splunk.com/application/splunk_process_injection_forwarder_bundle_downloads
Configure authentication for deployment servers and clients - Splunk Documentation	docs.splunk.com text/html	 CONFIRM docs.splunk.com/Documentation/Splunk/9.0.0/Security/ConfigDSDCAuthEnhancements#Configure_authentication_for_deployment_servers_and_clients_-_Splunk_Documentation
Security updates - Splunk Documentation	docs.splunk.com text/html	 CONFIRM docs.splunk.com/Documentation/Splunk/9.0.0/Security/Updates

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Splunk	Splunk	All	All	All	All
cpe:2.3:a:splunk:splunk:*:*:*:*:enterprise:*:*:						

Discovery Credit

Nadim Taha at Splunk

Social Mentions		
Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-32157 : Splunk Enterprise deployment servers in versions before 9.0 allow unauthenticated downloading of f... twitter.com/i/web/status/1...	2022-06-15 17:06:31
	Potentially Critical CVE Detected! CVE-2022-32157 Solunk Enterprise deploymnt servers in	2022-06-15

 @Robo_Alerts	...Security Critical CVE-2022-32157 CVE-2022-32158 CVE-2022-32159 Splunk Enterprise deployment servers in versions before 9.0 allow... twitter.com/i/web/status/1...	2022-06-16 18:56:01
 @ncsc_gov_ie	A number of vulnerabilities exists in Splunk Enterprise Deployment Servers, CVE-2022-32157 and CVE-2022-32158. For... twitter.com/i/web/status/1...	2022-06-17 10:08:48
 @RemotelyAlerts	Severity: ?? Splunk Enterprise deployment servers in ... CVE-2022-32157 Link for more: alerts.remotelyrmm.com/CVE-2022-32157	2022-06-24 02:33:15
 /r/netcve	CVE-2022-32157	2022-06-15 17:44:09

← Previous ID
Next ID →

© [CVE.report](#) 2023   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)