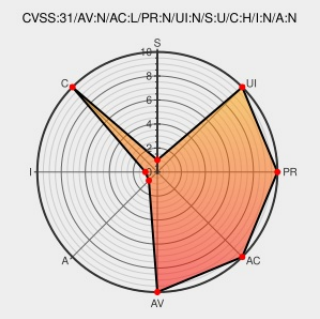
CVE-2022-32157

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/ConfigDSDCAuthEnhancements 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_downloa
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_a
Security updates - Splunk Documentation	docs.splunk.com text/html	CONFIRM docs.splunk.com/Documentation/Splunk/9.0.0/Security/Updates

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 Splunk Enterprise deployment servers in	2022-06-15

@Robo_Alerts	versions before 9.0 allow… twitter.com/i/web/status/1…	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→