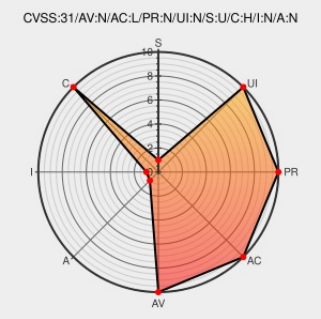
CVE-2022-32155

Published on: Not Yet Published

Last Modified on: 06/24/2022 01:21:00 AM UTC

CVE-2022-32155 - advisory for SVD-2022-0605

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Splunk from Splunk contain the following vulnerability:

In universal forwarder versions before 9.0, management services are available remotely by default. When not required, it introduces a potential exposure, but it is not a vulnerability. If exposed, we recommend each customer assess the potential severity specific to your environment. In 9.0, the universal forwarder now binds the management port to localhost preventing remote logins by default. If management services are not required in versions before 9.0, set disableDefaultPort = true in server.conf OR allowRemoteLogin = never in server.conf OR mgmtHostPort = localhost in web.conf. See Configure universal forwarder management security (https://docs.splunk.com/Documentation/Splunk/9.0.0/Security/EnableTLSCertHostnameValida for more information on disabling the remote management services.

CVE-2022-32155 has been assigned by prodsec@splunk.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Splunk, Inc** - **Universal Forwarder** 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	**Integrity**	**Availability**

Impact	Impact	Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Configure TLS certificate host name validation - Splunk Documentation	docs.splunk.com text/html	CONFIRM docs.splunk.com/Documentation/Splunk/9.0.0/Security/EnableTLSCertHostnameValidation#Configure_u
SVD-2022-0605 | Splunk	www.splunk.com text/html	CONFIRM www.splunk.com/en_us/product-security/announcements/svd-2022-0605.html
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
Application	Splunk	Splunk Cloud Platform	All	All	All	All

cpe:2.3:a:splunk:splunk:*:*:*:*:enterprise:*:*:*:

cpe:2.3:a:splunk:splunk_cloud_platform:*:*:*:*:*:*:*:*:

Discovery Credit

Chris Green at Splunk

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-32155 : In universal forwarder versions before 9.0, management services are available remotely by default.… twitter.com/i/web/status/1…	2022-06-15 17:05:45
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-32155 In universal forwarder versions before 9.0, management services a… twitter.com/i/web/status/1…	2022-06-15 18:56:01
@RemotelyAlerts	Severity: ?? | In universal forwarder versions before 9... | CVE-2022-32155 | Link for more: alerts.remotelyrmm.com/CVE-2022-32155	2022-06-24 02:32:03

/r/netcve	CVE-2022-32155	2022-06-15 17:44:07

← Previous ID

Next ID→