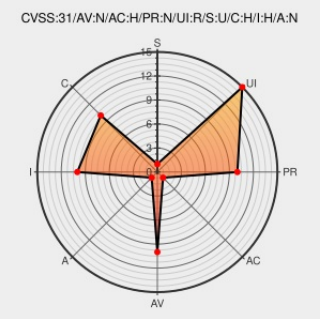
CVE-2022-32154

Published on: Not Yet Published

Last Modified on: 06/24/2022 01:22:00 AM UTC

CVE-2022-32154 - advisory for SVD-2022-0604

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



Certain versions of Splunk from Splunk contain the following vulnerability:

Dashboards in Splunk Enterprise versions before 9.0 might let an attacker inject risky search commands into a form token when the token is used in a query in a cross-origin request. The result bypasses SPL safeguards for risky commands. See New capabilities can limit access to some custom and potentially risky commands (https://docs.splunk.com/Documentation/Splunk/9.0.0/Security/SPLsafeguards#New_capabilitie for more information. Note that the attack is browser-based and an attacker cannot exploit it at will.

CVE-2022-32154 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**

Affected Vendor/Software: **Splunk, Inc** - **Splunk Cloud Platform** version **< 8.2.2106**

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

PARTIAL | PARTIAL | NONE

CVE References

Description	Tags	Link
Splunk Command and Scripting Interpreter Delete Usage - Splunk Security Content	research.splunk.com text/html	CONFIRM research.splunk.com/application/splunk_command_and_scripting_interpreter_delete_us
SVD-2022-0604 | Splunk	www.splunk.com text/html	CONFIRM www.splunk.com/en_us/product-security/announcements/svd-2022-0604.html
SPL safeguards for risky commands - Splunk Documentation	docs.splunk.com text/html	CONFIRM docs.splunk.com/Documentation/Splunk/9.0.0/Security/SPLsafeguards#New_capabilities_can_limit_a
Splunk Command and Scripting Interpreter Risky SPL MLTK - Splunk Security Content	research.splunk.com text/html	CONFIRM research.splunk.com/application/splunk_command_and_scripting_interpreter_risky_spl
Splunk Command and Scripting Interpreter Risky Commands - Splunk Security Content	research.splunk.com text/html	CONFIRM research.splunk.com/application/splunk_command_and_scripting_interpreter_risky_cor
Security updates - Splunk Documentation	docs.splunk.com text/html	CONFIRM docs.splunk.com/Documentation/Splunk/9.0.0/Security/Updates

Related QID Numbers

378025 Splunk Enterprise Search Injection Vulnerability (SVD-2022-0604)

378038 Splunk Enterprise Security Update (SVD-2022-0604)

730652 Splunk Enterprise Search Injection Vulnerability (SVD-2022-0604)

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

Danylo Dmytriiev (DDV_UA)

Anton (therceman)

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-32154 : Dashboards in Splunk Enterprise versions before 9.0 might let an attacker inject risky search comm… twitter.com/i/web/status/1…	2022-06-15 17:05:25
@therceman	Acknowledged by Splunk ?CVE-2022-32154 ?SVD-2022-0604 ? www.splunk .com/en_us/product-security/announcements/svd-… twitter.com/i/web/status/1…	2022-06-16 19:52:24
@RemotelyAlerts	Severity: ?? | Dashboards in Splunk Enterprise versions... | CVE-2022-32154 | Link for more: alerts.remotelyrmm.com/CVE-2022-32154	2022-06-24 02:31:27
/r/netcve	CVE-2022-32154	2022-06-15 17:44:06

← Previous ID

Next ID→