

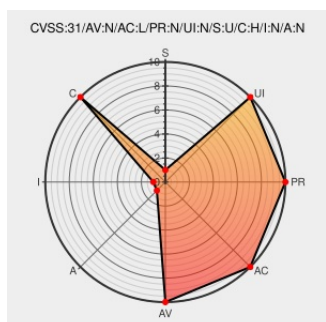


CVE-2022-32155

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

PARTIAL

Impact

NONE

Impact

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_hostname_validation
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

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
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

[← 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](#)