



CVE-2022-32151

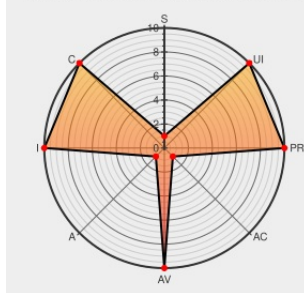
Published on: Not Yet Published

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

CVE-2022-32151 - advisory for SVD-2022-0601

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

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N



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

The `httplib` and `urllib` Python libraries that Splunk shipped with Splunk Enterprise did not validate certificates using the certificate authority (CA) certificate stores by default in Splunk Enterprise versions before 9.0 and Splunk Cloud Platform versions before 8.2.2203. Python 3 client libraries now verify server certificates by default and use the

appropriate CA certificate stores for each library. Apps and add-ons that include their own HTTP libraries are not affected. For Splunk Enterprise, update to Splunk Enterprise version 9.0 and Configure TLS host name validation for Splunk-to-Splunk communications (<https://docs.splunk.com/Documentation/Splunk/9.0.0/Security/EnableTLSCertHostnameValida>) to enable the remediation.

CVE-2022-32151 has been assigned by [prodsec@splunk.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

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

Affected Vendor/Software: [Splunk, Inc](#) - **Splunk Cloud Platform** version < 8.2.2203

CVSS3 Score: **9.1 - CRITICAL**

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

CVSS2 Score: **6.4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Splunk protocol impersonation weak encryption simplerequest - Splunk Security Content	research.splunk.com text/html	 CONFIRM research.splunk.com/application/splunk_protocol_impersonation_weak_encryption_simplerequest/
Configure TLS certificate host name validation - Splunk Documentation	docs.splunk.com text/html	 CONFIRM docs.splunk.com/Documentation/Splunk/9.0.0/Security/EnableTLSCertHostnameValidation
SVD-2022-0601 Splunk	www.splunk.com text/html	 CONFIRM www.splunk.com/en_us/product-security/announcements/svd-2022-0601.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-2022-32151 : The httpLib and urllib Python libraries that Splunk shipped with Splunk Enterprise did not validat... twitter.com/i/web/status/1...	2022-06-15 17:04:34

 @RemotelyAlerts	Severity: ?? The httpLib and urllib Python libraries ... CVE-2022-32151 Link for more: alerts.remotelyrmm.com/CVE-2022-32151	2022-06-24 02:30:16
 /r/netcve	CVE-2022-32151	2022-06-15 17:44:03

[← 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](#)