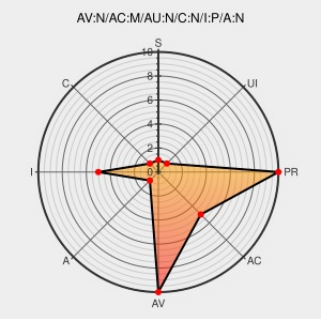
CVE-2015-6514

Published on: 08/18/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:16 PM UTC

CVE-2015-6514

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



Certain versions of Splunk from Splunk contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in the Dashboard in Splunk Enterprise 6.2.x before 6.2.4 and Splunk Light 6.2.x before 6.2.4 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.

CVE-2015-6514 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Splunk Enterprise 6.2.4 and Splunk Light 6.2.4 address two vulnerabilities | Splunk	Vendor Advisory, www.splunk.com, text/html	CONFIRM www.splunk.com/view/SP-CAAAN7C
Splunk Enterprise and Splunk Light Input Validation Flaw Lets Remote Users Conduct Cross-Site Scripting Attacks - SecurityTracker	www.securitytracker.com, text/html	SECTRACK 1032859

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	6.2.0	All	All	All
Application	Splunk	Splunk	6.2.0	All	All	All
Application	Splunk	Splunk	6.2.1	All	All	All
Application	Splunk	Splunk	6.2.1	All	All	All
Application	Splunk	Splunk	6.2.2	All	All	All
Application	Splunk	Splunk	6.2.2	All	All	All
Application	Splunk	Splunk	6.2.3	All	All	All
Application	Splunk	Splunk	6.2.3	All	All	All
Application	Splunk	Splunk	6.2.0	All	All	All
Application	Splunk	Splunk	6.2.0	All	All	All
Application	Splunk	Splunk	6.2.1	All	All	All
Application	Splunk	Splunk	6.2.1	All	All	All
Application	Splunk	Splunk	6.2.2	All	All	All
Application	Splunk	Splunk	6.2.2	All	All	All
Application	Splunk	Splunk	6.2.3	All	All	All
Application	Splunk	Splunk	6.2.3	All	All	All

cpe:2.3:a:splunk:splunk:6.2.0:*:*:*:enterprise:*:*:*:

cpe:2.3:a:splunk:splunk:6.2.0:*:*:*:light:*:*:*:

cpe:2.3:a:splunk:splunk:6.2.1:*:*:*:enterprise:*:*:*:

cpe:2.3:a:splunk:splunk:6.2.1:*:*:*:light:*:*:*:

cpe:2.3:a:splunk:splunk:6.2.2:*:*:*:enterprise:*:*:*:

cpe:2.3:a:splunk:splunk:6.2.2:*:*:*:light:*:*:*:

cpe:2.3:a:splunk:splunk:6.2.3:*:*:*:enterprise:*:*:*:

cpe:2.3:a:splunk:splunk:6.2.3:*:*:*:light:*:*:*:

cpe:2.3:a:splunk:splunk:6.2.0:*:*:*:enterprise:*:*:*:

cpe:2.3:a:splunk:splunk:6.2.0:*:*:*:light:*:*:*:

cpe:2.3:a:splunk:splunk:6.2.1:*:*:*:enterprise:*:*:*:

cpe:2.3:a:splunk:splunk:6.2.1:*:*:*:light:*:*:*:

cpe:2.3:a:splunk:splunk:6.2.2:*:*:*:enterprise:*:*:*:

cpe:2.3:a:splunk:splunk:6.2.2:*:*:*:light:*:*:*:

cpe:2.3:a:splunk:splunk:6.2.3:*:*:*:enterprise:*:*:*:

cpe:2.3:a:splunk:splunk:6.2.3:*:*:*:light:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→