



CVE-2014-8303

Published on: 10/16/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:51 PM UTC

CVE-2014-8303

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Cross-site scripting (XSS) vulnerability in Splunk Web in Splunk Enterprise 6.1.x before 6.1.4 and 6.0.x before 6.0.6 allows remote attackers to inject arbitrary web script or HTML via vectors related to event parsing.

CVE-2014-8303 has been assigned by [M](#) 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 Input Validation Flaws Permits Cross-Site Scripting Attacks - SecurityTracker

www.securitytracker.com
text/html

[SECTrack 1030994](https://sectrack.com/1030994)

Splunk Enterprise 6.1.4 and 5.0.10 address four vulnerabilities | Splunk

[Vendor Advisory](#)
www.splunk.com
text/html

[CONFIRM
www.splunk.com/view/SP-CAAANHS](https://www.splunk.com/view/SP-CAAANHS)

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	6.0	All	All	All
Application	Splunk	Splunk	6.0.1	All	All	All
Application	Splunk	Splunk	6.0.2	All	All	All
Application	Splunk	Splunk	6.0.3	All	All	All
Application	Splunk	Splunk	6.0.4	All	All	All
Application	Splunk	Splunk	6.0.5	All	All	All
Application	Splunk	Splunk	6.1	All	All	All
Application	Splunk	Splunk	6.1.1	All	All	All
Application	Splunk	Splunk	6.1.2	All	All	All
Application	Splunk	Splunk	6.1.3	All	All	All
Application	Splunk	Splunk	6.0	All	All	All
Application	Splunk	Splunk	6.0.1	All	All	All
Application	Splunk	Splunk	6.0.2	All	All	All
Application	Splunk	Splunk	6.0.3	All	All	All
Application	Splunk	Splunk	6.0.4	All	All	All
Application	Splunk	Splunk	6.0.5	All	All	All
Application	Splunk	Splunk	6.1	All	All	All
Application	Splunk	Splunk	6.1.1	All	All	All
Application	Splunk	Splunk	6.1.2	All	All	All
Application	Splunk	Splunk	6.1.3	All	All	All
cpe:2.3:a:splunk:splunk:6.0:****.*.*.*:						
cpe:2.3:a:splunk:splunk:6.0.1:****.*.*.*:						
cpe:2.3:a:splunk:splunk:6.0.2:****.*.*.*:						
cpe:2.3:a:splunk:splunk:6.0.3:****.*.*.*:						
cpe:2.3:a:splunk:splunk:6.0.4:****.*.*.*:						
cpe:2.3:a:splunk:splunk:6.0.5:****.*.*.*:						
cpe:2.3:a:splunk:splunk:6.1:***.enterprise:***:						
cpe:2.3:a:splunk:splunk:6.1.1:***.enterprise:***:						
cpe:2.3:a:splunk:splunk:6.1.2:***.enterprise:***:						
cpe:2.3:a:splunk:splunk:6.1.3:***.enterprise:***:						

cpe:2.3:a:splunk:splunk:6.0:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:6.0.1:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:6.0.2:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:6.0.3:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:6.0.4:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:6.0.5:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:6.1:*:*:*enterprise:*:*:
cpe:2.3:a:splunk:splunk:6.1.1:*:*:*enterprise:*:*:
cpe:2.3:a:splunk:splunk:6.1.2:*:*:*enterprise:*:*:
cpe:2.3:a:splunk:splunk:6.1.3:*:*:*enterprise:*:*:

No vendor comments have been submitted for this CVE