



CVE-2010-2503

Published on: 06/28/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:10 PM UTC

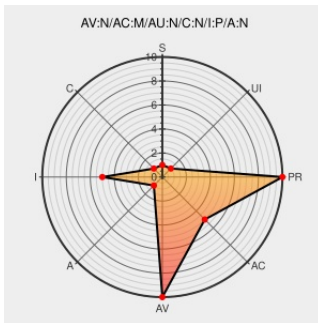
CVE-2010-2503

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Multiple cross-site scripting (XSS) vulnerabilities in Splunk 4.0 through 4.0.10 and 4.1 through 4.1.1 allow remote attackers to inject arbitrary web script or HTML via (1) redirects, aka SPL-31067; (2) unspecified "user->user or user->admin" vectors, aka SPL-31084; or (3) unspecified "user input," aka SPL-31085.

CVE-2010-2503 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector

NETWORK

Access Complexity

MEDIUM

Authentication

NONE

Confidentiality Impact

NONE

Integrity Impact

PARTIAL

Availability Impact

NONE

CVE References

Description

Splunk : Splunk Critical Maintenance Release and Patch - May 3rd, 2010

Tags

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

Link

[CONFIRM](#) www.splunk.com/view/SP-CAAAGD

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 CIDs associated with this CVE

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	4.0	All	All	All
Application	Splunk	Splunk	4.0.1	All	All	All
Application	Splunk	Splunk	4.0.10	All	All	All
Application	Splunk	Splunk	4.0.2	All	All	All
Application	Splunk	Splunk	4.0.3	All	All	All
Application	Splunk	Splunk	4.0.4	All	All	All
Application	Splunk	Splunk	4.0.5	All	All	All
Application	Splunk	Splunk	4.0.6	All	All	All
Application	Splunk	Splunk	4.0.7	All	All	All
Application	Splunk	Splunk	4.0.8	All	All	All
Application	Splunk	Splunk	4.0.9	All	All	All
Application	Splunk	Splunk	4.1	All	All	All
Application	Splunk	Splunk	4.1.1	All	All	All
Application	Splunk	Splunk	4.0	All	All	All
Application	Splunk	Splunk	4.0.1	All	All	All
Application	Splunk	Splunk	4.0.10	All	All	All
Application	Splunk	Splunk	4.0.2	All	All	All
Application	Splunk	Splunk	4.0.3	All	All	All
Application	Splunk	Splunk	4.0.4	All	All	All
Application	Splunk	Splunk	4.0.5	All	All	All
Application	Splunk	Splunk	4.0.6	All	All	All
Application	Splunk	Splunk	4.0.7	All	All	All
Application	Splunk	Splunk	4.0.8	All	All	All
Application	Splunk	Splunk	4.0.9	All	All	All
Application	Splunk	Splunk	4.1	All	All	All
Application	Splunk	Splunk	4.1.1	All	All	All
cpe:2.3:a:splunk:splunk:4.0:*****:						
cpe:2.3:a:splunk:splunk:4.0.1:*****:						
cpe:2.3:a:splunk:splunk:4.0.10:*****:						
cpe:2.3:a:splunk:splunk:4.0.2:*****:						
cpe:2.3:a:splunk:splunk:4.0.3:*****:						

cpe:2.3:a:splunk:splunk:4.0.4:*****:
cpe:2.3:a:splunk:splunk:4.0.5:*****:
cpe:2.3:a:splunk:splunk:4.0.6:*****:
cpe:2.3:a:splunk:splunk:4.0.7:*****:
cpe:2.3:a:splunk:splunk:4.0.8:*****:
cpe:2.3:a:splunk:splunk:4.0.9:*****:
cpe:2.3:a:splunk:splunk:4.1:*****:
cpe:2.3:a:splunk:splunk:4.1.1:*****:
cpe:2.3:a:splunk:splunk:4.0:*****:
cpe:2.3:a:splunk:splunk:4.0.1:*****:
cpe:2.3:a:splunk:splunk:4.0.10:*****:
cpe:2.3:a:splunk:splunk:4.0.2:*****:
cpe:2.3:a:splunk:splunk:4.0.3:*****:
cpe:2.3:a:splunk:splunk:4.0.4:*****:
cpe:2.3:a:splunk:splunk:4.0.5:*****:
cpe:2.3:a:splunk:splunk:4.0.6:*****:
cpe:2.3:a:splunk:splunk:4.0.7:*****:
cpe:2.3:a:splunk:splunk:4.0.8:*****:
cpe:2.3:a:splunk:splunk:4.0.9:*****:
cpe:2.3:a:splunk:splunk:4.1:*****:
cpe:2.3:a:splunk:splunk:4.1.1:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

[site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report