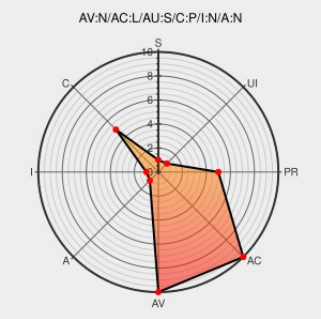
CVE-2011-4643

Published on: 01/03/2012 12:00:00 AM UTC

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

CVE-2011-4643

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



Certain versions of Splunk from Splunk contain the following vulnerability:

Multiple directory traversal vulnerabilities in Splunk 4.x before 4.2.5 allow remote authenticated users to read arbitrary files via a .. (dot dot) in a URI to (1) Splunk Web or (2) the Splunkd HTTP Server, aka SPL-45243.

CVE-2011-4643 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Sec-1 now fully incorporated into Claranet. How to find us. | Claranet UK	Exploit, www.sec-1.com, application/pdf	MISC www.sec-1.com/blog/wp-content/uploads/2011/12/Attacking_Splunk_Release.pdf
Advisory: Multiple Splunk Vulnerabilities | Sec-1 Labs	www.sec-1.com, text/html	MISC www.sec-1.com/blog/?p=233
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF splunk-splunkd-directory-traversal(72244)
Splunk Remote Root Exploit	Exploit, www.exploit-db.com, Proof of Concept, text/x-python	EXPLOIT-DB 18245
Splunk Bugs Permit Remote Autheticated Code Injection and Directory Traversal and Remote	www.securitytracker.com, text/html	SECTRACK 1026451

Cross-Site Scripting Attacks - SecurityTracker		
Security Alerts - Secunia	web.archive.org text/html	SECUNIA 47232
Splunk 4.2.5 addresses three vulnerabilities - December 12th, 2011 | Splunk	Vendor Advisory www.splunk.com text/html	CONFIRM www.splunk.com/view/SP-CAAAGMM

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	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	4.0.11	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	4.1.2	All	All	All
Application	Splunk	Splunk	4.1.3	All	All	All
Application	Splunk	Splunk	4.1.4	All	All	All
Application	Splunk	Splunk	4.1.5	All	All	All
Application	Splunk	Splunk	4.1.6	All	All	All
Application	Splunk	Splunk	4.1.7	All	All	All
Application	Splunk	Splunk	4.1.8	All	All	All
Application	Splunk	Splunk	4.2	All	All	All
Application	Splunk	Splunk	4.2.1	All	All	All

Application	Splunk	Splunk	4.2.2	All	All	All
Application	Splunk	Splunk	4.2.3	All	All	All
Application	Splunk	Splunk	4.2.4	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	4.0.11	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	4.1.2	All	All	All
Application	Splunk	Splunk	4.1.3	All	All	All
Application	Splunk	Splunk	4.1.4	All	All	All
Application	Splunk	Splunk	4.1.5	All	All	All
Application	Splunk	Splunk	4.1.6	All	All	All
Application	Splunk	Splunk	4.1.7	All	All	All
Application	Splunk	Splunk	4.1.8	All	All	All
Application	Splunk	Splunk	4.2	All	All	All
Application	Splunk	Splunk	4.2.1	All	All	All
Application	Splunk	Splunk	4.2.2	All	All	All
Application	Splunk	Splunk	4.2.3	All	All	All
Application	Splunk	Splunk	4.2.4	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:4.0.11:*:*:*:*:*:*:*:

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:4.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.1.6:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.1.7:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.1.8:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.2:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.2.4:*:*:*:*:*:*:*:

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:4.0.11:*:*:*:*:*:*:*:

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:4.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.1.6:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.1.7:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.1.8:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.2:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:splunk:splunk:4.2.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→