



CVE-2011-4644

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

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

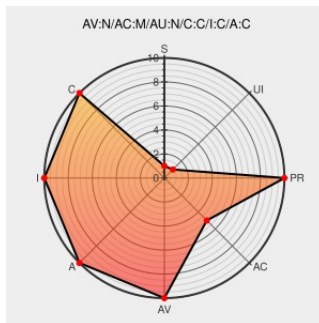
CVE-2011-4644

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Splunk 4.2.5 and earlier, when a Free license is selected, enables potentially undesirable functionality within an environment that intentionally does not support authentication, which allows remote attackers to (1) read arbitrary files via a management-console session that leverages the ability to create crafted data sources, or (2) execute management commands via an HTTP request.

CVE-2011-4644 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **9.3 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

COMPLETE

COMPLETE

COMPLETE

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

Exploit
[www.sec-1.com](#)
[text/html](#)

MISC [www.sec-1.com/blog/?p=233](#)

Splunk Remote Root Exploit

Exploit
[www.exploit-db.com](#)
Proof of Concept
[text/x-python](#)

EXPLOIT-DB 18245

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	2.1	All	All	All
Application	Splunk	Splunk	2.2	All	All	All
Application	Splunk	Splunk	2.2.1	All	All	All
Application	Splunk	Splunk	2.2.3	All	All	All
Application	Splunk	Splunk	2.2.6	All	All	All
Application	Splunk	Splunk	3.0	All	All	All
Application	Splunk	Splunk	3.0.1	All	All	All
Application	Splunk	Splunk	3.0.2	All	All	All
Application	Splunk	Splunk	3.1	All	All	All
Application	Splunk	Splunk	3.1.1	All	All	All
Application	Splunk	Splunk	3.1.2	All	All	All
Application	Splunk	Splunk	3.1.3	All	All	All
Application	Splunk	Splunk	3.1.4	All	All	All
Application	Splunk	Splunk	3.2	All	All	All
Application	Splunk	Splunk	3.2.1	All	All	All
Application	Splunk	Splunk	3.2.2	All	All	All
Application	Splunk	Splunk	3.2.3	All	All	All
Application	Splunk	Splunk	3.2.4	All	All	All
Application	Splunk	Splunk	3.2.5	All	All	All
Application	Splunk	Splunk	3.2.6	All	All	All
Application	Splunk	Splunk	3.3	All	All	All
Application	Splunk	Splunk	3.3.1	All	All	All
Application	Splunk	Splunk	3.3.2	All	All	All
Application	Splunk	Splunk	3.3.3	All	All	All
Application	Splunk	Splunk	3.3.4	All	All	All
Application	Splunk	Splunk	3.4	All	All	All
Application	Splunk	Splunk	3.4.1	All	All	All
Application	Splunk	Splunk	3.4.10	All	All	All

Application	Splunk	Splunk	3.4.11	All	All	All
Application	Splunk	Splunk	3.4.12	All	All	All
Application	Splunk	Splunk	3.4.13	All	All	All
Application	Splunk	Splunk	3.4.14	All	All	All
Application	Splunk	Splunk	3.4.2	All	All	All
Application	Splunk	Splunk	3.4.3	All	All	All
Application	Splunk	Splunk	3.4.5	All	All	All
Application	Splunk	Splunk	3.4.6	All	All	All
Application	Splunk	Splunk	3.4.8	All	All	All
Application	Splunk	Splunk	3.4.9	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

Application	Splunk	Splunk	4.2.4	All	All	All
Application	Splunk	Splunk	2.1	All	All	All
Application	Splunk	Splunk	2.2	All	All	All
Application	Splunk	Splunk	2.2.1	All	All	All
Application	Splunk	Splunk	2.2.3	All	All	All
Application	Splunk	Splunk	2.2.6	All	All	All
Application	Splunk	Splunk	3.0	All	All	All
Application	Splunk	Splunk	3.0.1	All	All	All
Application	Splunk	Splunk	3.0.2	All	All	All
Application	Splunk	Splunk	3.1	All	All	All
Application	Splunk	Splunk	3.1.1	All	All	All
Application	Splunk	Splunk	3.1.2	All	All	All
Application	Splunk	Splunk	3.1.3	All	All	All
Application	Splunk	Splunk	3.1.4	All	All	All
Application	Splunk	Splunk	3.2	All	All	All
Application	Splunk	Splunk	3.2.1	All	All	All
Application	Splunk	Splunk	3.2.2	All	All	All
Application	Splunk	Splunk	3.2.3	All	All	All
Application	Splunk	Splunk	3.2.4	All	All	All
Application	Splunk	Splunk	3.2.5	All	All	All
Application	Splunk	Splunk	3.2.6	All	All	All
Application	Splunk	Splunk	3.3	All	All	All
Application	Splunk	Splunk	3.3.1	All	All	All
Application	Splunk	Splunk	3.3.2	All	All	All
Application	Splunk	Splunk	3.3.3	All	All	All
Application	Splunk	Splunk	3.3.4	All	All	All
Application	Splunk	Splunk	3.4	All	All	All
Application	Splunk	Splunk	3.4.1	All	All	All
Application	Splunk	Splunk	3.4.10	All	All	All
Application	Splunk	Splunk	3.4.11	All	All	All
Application	Splunk	Splunk	3.4.12	All	All	All
Application	Splunk	Splunk	3.4.13	All	All	All
Application	Splunk	Splunk	3.4.14	All	All	All
Application	Splunk	Splunk	3.4.2	All	All	All
Application	Splunk	Splunk	3.4.3	All	All	All
Application	Splunk	Splunk	3.4.5	All	All	All

Application	Splunk	Splunk	3.4.6	All	All	All
Application	Splunk	Splunk	3.4.8	All	All	All
Application	Splunk	Splunk	3.4.9	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
Application	Splunk	Splunk	All	All	All	All
cpe:2.3:a:splunk:splunk:2.1:*****:						
cpe:2.3:a:splunk:splunk:2.2:*****:						
cpe:2.3:a:splunk:splunk:2.2.1:*****:						
cpe:2.3:a:splunk:splunk:2.2.3:*****:						

cpe:2.3:a:splunk:splunk:2.2.6:*****:
cpe:2.3:a:splunk:splunk:3.0:*****:
cpe:2.3:a:splunk:splunk:3.0.1:*****:
cpe:2.3:a:splunk:splunk:3.0.2:*****:
cpe:2.3:a:splunk:splunk:3.1:*****:
cpe:2.3:a:splunk:splunk:3.1.1:*****:
cpe:2.3:a:splunk:splunk:3.1.2:*****:
cpe:2.3:a:splunk:splunk:3.1.3:*****:
cpe:2.3:a:splunk:splunk:3.1.4:*****:
cpe:2.3:a:splunk:splunk:3.2:*****:
cpe:2.3:a:splunk:splunk:3.2.1:*****:
cpe:2.3:a:splunk:splunk:3.2.2:*****:
cpe:2.3:a:splunk:splunk:3.2.3:*****:
cpe:2.3:a:splunk:splunk:3.2.4:*****:
cpe:2.3:a:splunk:splunk:3.2.5:*****:
cpe:2.3:a:splunk:splunk:3.2.6:*****:
cpe:2.3:a:splunk:splunk:3.3:*****:
cpe:2.3:a:splunk:splunk:3.3.1:*****:
cpe:2.3:a:splunk:splunk:3.3.2:*****:
cpe:2.3:a:splunk:splunk:3.3.3:*****:
cpe:2.3:a:splunk:splunk:3.3.4:*****:
cpe:2.3:a:splunk:splunk:3.4:*****:
cpe:2.3:a:splunk:splunk:3.4.1:*****:
cpe:2.3:a:splunk:splunk:3.4.10:*****:
cpe:2.3:a:splunk:splunk:3.4.11:*****:
cpe:2.3:a:splunk:splunk:3.4.12:*****:
cpe:2.3:a:splunk:splunk:3.4.13:*****:
cpe:2.3:a:splunk:splunk:3.4.14:*****:
cpe:2.3:a:splunk:splunk:3.4.2:*****:

cpe:2.3:a:splunk:splunk:3.4.2:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:3.4.3:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:3.4.5:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:3.4.6:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:3.4.8:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:3.4.9:*:*:*:*:*:
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:2.1:*****:
cpe:2.3:a:splunk:splunk:2.2:*****:
cpe:2.3:a:splunk:splunk:2.2.1:*****:
cpe:2.3:a:splunk:splunk:2.2.3:*****:
cpe:2.3:a:splunk:splunk:2.2.6:*****:
cpe:2.3:a:splunk:splunk:3.0:*****:
cpe:2.3:a:splunk:splunk:3.0.1:*****:
cpe:2.3:a:splunk:splunk:3.0.2:*****:
cpe:2.3:a:splunk:splunk:3.1:*****:
cpe:2.3:a:splunk:splunk:3.1.1:*****:
cpe:2.3:a:splunk:splunk:3.1.2:*****:
cpe:2.3:a:splunk:splunk:3.1.3:*****:
cpe:2.3:a:splunk:splunk:3.1.4:*****:
cpe:2.3:a:splunk:splunk:3.2:*****:
cpe:2.3:a:splunk:splunk:3.2.1:*****:
cpe:2.3:a:splunk:splunk:3.2.2:*****:
cpe:2.3:a:splunk:splunk:3.2.3:*****:
cpe:2.3:a:splunk:splunk:3.2.4:*****:
cpe:2.3:a:splunk:splunk:3.2.5:*****:
cpe:2.3:a:splunk:splunk:3.2.6:*****:
cpe:2.3:a:splunk:splunk:3.3:*****:
cpe:2.3:a:splunk:splunk:3.3.1:*****:
cpe:2.3:a:splunk:splunk:3.3.2:*****:
cpe:2.3:a:splunk:splunk:3.3.3:*****:
cpe:2.3:a:splunk:splunk:3.3.4:*****:
cpe:2.3:a:splunk:splunk:3.3.5:*****:

cpe:2.3:a:splunk:splunk:3.4:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:3.4.1:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:3.4.10:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:3.4.11:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:3.4.12:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:3.4.13:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:3.4.14:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:3.4.2:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:3.4.3:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:3.4.5:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:3.4.6:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:3.4.8:*:*:*:*:*:
cpe:2.3:a:splunk:splunk:3.4.9:*:*:*:*:*:
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:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)