

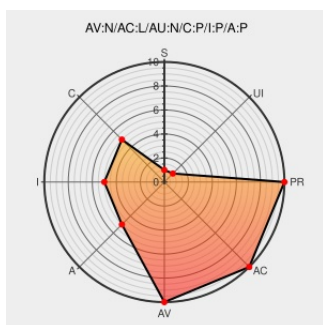


CVE-2013-1435

Published on: 08/23/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:33 PM UTC

CVE-2013-1435

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

(1) snmp.php and (2) rrd.php in Cacti before 0.8.8b allows remote attackers to execute arbitrary commands via shell metacharacters in unspecified vectors.

CVE-2013-1435 has been assigned by security@debian.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

No Description Provided

[Patch](#)

[svn.cacti.net](#)

[CONFIRM svn.cacti.net/viewvc?view=rev&revision=7393](#)

Inactive Link **Not Archived**

oss-security - Re: CVE request: SQL injection and shell escaping issues in Cacti < 0.8.8b

[www.openwall.com](#)

[text/html](#)

[MLIST \[oss-security\] 20130807 Re: CVE request: SQL injection and shell escaping issues in Cacti < 0.8.8b](#)

openSUSE-SU-2013:1377-1: moderate: cacti: security and bugfix update to

[lists.opensuse.org](#)

[text/html](#)

[SUSE openSUSE-SU-2013:1377](#)

Debian -- Page not found

[www.debian.org](#)

Deprecated Link

[text/html](#)

Inactive Link **Not Archived**

[DEBIAN DSA-2739](#)

About Secunia Research Flexera	secunia.com Deprecated Link text/plain	SECUNIA 54181
No Description Provided	svn.cacti.net Inactive Link Not Archived	CONFIRM svn.cacti.net/viewvc?view=rev&revision=7392
Cacti • View topic - Release of Cacti 0.8.8b	forums.cacti.net text/html	CONFIRM forums.cacti.net/viewtopic.php?f=21&t=50593
About Secunia Research Flexera	Vendor Advisory secunia.com Deprecated Link text/plain	SECUNIA 54386

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	Cacti	Cacti	0.8	All	All	All
Application	Cacti	Cacti	0.8.1	All	All	All
Application	Cacti	Cacti	0.8.2	All	All	All
Application	Cacti	Cacti	0.8.2a	All	All	All
Application	Cacti	Cacti	0.8.3	All	All	All
Application	Cacti	Cacti	0.8.3a	All	All	All
Application	Cacti	Cacti	0.8.4	All	All	All
Application	Cacti	Cacti	0.8.5	All	All	All
Application	Cacti	Cacti	0.8.5a	All	All	All
Application	Cacti	Cacti	0.8.6	All	All	All
Application	Cacti	Cacti	0.8.6a	All	All	All
Application	Cacti	Cacti	0.8.6b	All	All	All
Application	Cacti	Cacti	0.8.6c	All	All	All
Application	Cacti	Cacti	0.8.6d	All	All	All
Application	Cacti	Cacti	0.8.6e	All	All	All
Application	Cacti	Cacti	0.8.6f	All	All	All
Application	Cacti	Cacti	0.8.6g	All	All	All
Application	Cacti	Cacti	0.8.6h	All	All	All
Application	Cacti	Cacti	0.8.6i	All	All	All

Application	Cacti	Cacti	0.8.6j	All	All	All
Application	Cacti	Cacti	0.8.6k	All	All	All
Application	Cacti	Cacti	0.8.7	All	All	All
Application	Cacti	Cacti	0.8.7a	All	All	All
Application	Cacti	Cacti	0.8.7b	All	All	All
Application	Cacti	Cacti	0.8.7c	All	All	All
Application	Cacti	Cacti	0.8.7d	All	All	All
Application	Cacti	Cacti	0.8.7e	All	All	All
Application	Cacti	Cacti	0.8.7f	All	All	All
Application	Cacti	Cacti	0.8.7g	All	All	All
Application	Cacti	Cacti	0.8.7h	All	All	All
Application	Cacti	Cacti	0.8.7i	All	All	All
Application	Cacti	Cacti	0.8.8	All	All	All
Application	Cacti	Cacti	0.8.8a	All	All	All
Application	Cacti	Cacti	0.8	All	All	All
Application	Cacti	Cacti	0.8.1	All	All	All
Application	Cacti	Cacti	0.8.2	All	All	All
Application	Cacti	Cacti	0.8.2a	All	All	All
Application	Cacti	Cacti	0.8.3	All	All	All
Application	Cacti	Cacti	0.8.3a	All	All	All
Application	Cacti	Cacti	0.8.4	All	All	All
Application	Cacti	Cacti	0.8.5	All	All	All
Application	Cacti	Cacti	0.8.5a	All	All	All
Application	Cacti	Cacti	0.8.6	All	All	All
Application	Cacti	Cacti	0.8.6a	All	All	All
Application	Cacti	Cacti	0.8.6b	All	All	All
Application	Cacti	Cacti	0.8.6c	All	All	All
Application	Cacti	Cacti	0.8.6d	All	All	All
Application	Cacti	Cacti	0.8.6e	All	All	All
Application	Cacti	Cacti	0.8.6f	All	All	All
Application	Cacti	Cacti	0.8.6g	All	All	All
Application	Cacti	Cacti	0.8.6h	All	All	All
Application	Cacti	Cacti	0.8.6i	All	All	All
Application	Cacti	Cacti	0.8.6j	All	All	All
Application	Cacti	Cacti	0.8.6k	All	All	All
Application	Cacti	Cacti	0.8.7	All	All	All

Application	Cacti	Cacti	0.8.7a	All	All	All
Application	Cacti	Cacti	0.8.7b	All	All	All
Application	Cacti	Cacti	0.8.7c	All	All	All
Application	Cacti	Cacti	0.8.7d	All	All	All
Application	Cacti	Cacti	0.8.7e	All	All	All
Application	Cacti	Cacti	0.8.7f	All	All	All
Application	Cacti	Cacti	0.8.7g	All	All	All
Application	Cacti	Cacti	0.8.7h	All	All	All
Application	Cacti	Cacti	0.8.7i	All	All	All
Application	Cacti	Cacti	0.8.8	All	All	All
Application	Cacti	Cacti	0.8.8a	All	All	All
cpe:2.3:a:cacti:cacti:0.8:*****:						
cpe:2.3:a:cacti:cacti:0.8.1:*****:						
cpe:2.3:a:cacti:cacti:0.8.2:*****:						
cpe:2.3:a:cacti:cacti:0.8.2a:*****:						
cpe:2.3:a:cacti:cacti:0.8.3:*****:						
cpe:2.3:a:cacti:cacti:0.8.3a:*****:						
cpe:2.3:a:cacti:cacti:0.8.4:*****:						
cpe:2.3:a:cacti:cacti:0.8.5:*****:						
cpe:2.3:a:cacti:cacti:0.8.5a:*****:						
cpe:2.3:a:cacti:cacti:0.8.6:*****:						
cpe:2.3:a:cacti:cacti:0.8.6a:*****:						
cpe:2.3:a:cacti:cacti:0.8.6b:*****:						
cpe:2.3:a:cacti:cacti:0.8.6c:*****:						
cpe:2.3:a:cacti:cacti:0.8.6d:*****:						
cpe:2.3:a:cacti:cacti:0.8.6e:*****:						
cpe:2.3:a:cacti:cacti:0.8.6f:*****:						
cpe:2.3:a:cacti:cacti:0.8.6g:*****:						
cpe:2.3:a:cacti:cacti:0.8.6h:*****:						
cpe:2.3:a:cacti:cacti:0.8.6i:*****:						

cpe:2.3:a:cacti:cacti:0.8.6j:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.8.6k:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.8.7:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.8.7a:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.8.7b:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.8.7c:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.8.7d:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.8.7e:*.:.:.:.:.:.:

cpe:2.3:a:cacti:cacti:0.8.7f:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.8.7g:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.8.7h:*:*:*:*:*:*:

```
cpe:2.3:a:cacti:cacti:0.8.7i:*:*:*:*:*:*:
```

```
cpe:2.3:a:cacti:cacti:0.8.8:*:*:*:*:*:*:*:
```

cpe:2.3:a:cacti:cacti:0.8.8a:*:*:*:*:*:*:

```
cpe:2.3:a:cacti:cacti:0.8:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:cacti:cacti:0.8.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:cacti:cacti:0.8.2:*:*:*:*:*:*:
```

cpe:2.3:a:cacti:cacti:0.8.2a:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.8.3:*:*:*:*:*:*:

```
cpe:2.3:a:cacti:cacti:0.8.3a:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:cacti:cacti:0.8.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:cacti:cacti:0.8.5:*:*:*:*:*:*:
```

cpe:2.3:a:cacti:cacti:0.8.5a:*:*:*:*:*:*:

```
cpe:2.3:a:cacti:cacti:0.8.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:cacti:cacti:0.8.6a:*:*:*:*:*:*:*:
```

cpe:2.3:a:cacti:cacti:0.8.6b:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.8.6c:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.8.6d:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.8.6e:*:*:*:*:*:*:

