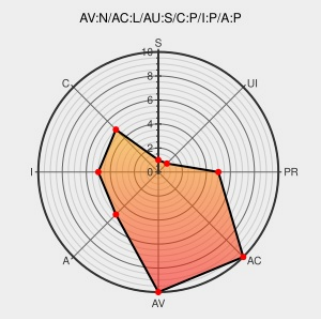
CVE-2010-1645

Published on: 08/23/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:18 AM UTC

CVE-2010-1645

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



Certain versions of Cacti from Cacti contain the following vulnerability:

Cacti before 0.8.7f, as used in Red Hat High Performance Computing (HPC) Solution and other products, allows remote authenticated administrators to execute arbitrary commands via shell metacharacters in (1) the FQDN field of a Device or (2) the Vertical Label field of a Graph Template.

CVE-2010-1645 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Bug 609115 – CVE-2010-1645 cacti: multiple command injection flaws (BONSAI-2010-0105)	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=609115
Cacti: The Complete RRDTool-based Graphing Solution	www.cacti.net text/html	CONFIRM www.cacti.net/release_notes_0_8_7f.php
:: Vulnerability Research ::	web.archive.org text/html Inactive Link Not Archived	MISC www.bonsai-sec.com/en/research/vulnerabilities/cacti-os-command-injection-0105.php
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2010:0635
Support / Security / Advisories / / MDVSA-2010:160 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2010:160

Red Hat High Performance Computing (HPC) Solution Multiple Vulnerabilities - Advisories - Community	Vendor Advisory web.archive.org text/html	SECUNIA 41041
No Description Provided	svn.cacti.net Inactive Link Not Archived	CONFIRM svn.cacti.net/viewvc?view=rev&revision=5778
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2010-2132
No Description Provided	svn.cacti.net Inactive Link Not Archived	CONFIRM svn.cacti.net/viewvc?view=rev&revision=5782
No Description Provided	svn.cacti.net Inactive Link Not Archived	CONFIRM svn.cacti.net/viewvc?view=rev&revision=5784

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	0.5	-	All	All
Application	Cacti	Cacti	0.6	All	All	All
Application	Cacti	Cacti	0.6.1	All	All	All
Application	Cacti	Cacti	0.6.2	All	All	All
Application	Cacti	Cacti	0.6.3	All	All	All
Application	Cacti	Cacti	0.6.4	All	All	All
Application	Cacti	Cacti	0.6.5	All	All	All
Application	Cacti	Cacti	0.6.6	All	All	All
Application	Cacti	Cacti	0.6.7	All	All	All
Application	Cacti	Cacti	0.6.8	All	All	All
Application	Cacti	Cacti	0.6.8a	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	0.8.6f	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	All	All	All	All
Application	Cacti	Cacti	0.5	-	All	All
Application	Cacti	Cacti	0.6	All	All	All
Application	Cacti	Cacti	0.6.1	All	All	All
Application	Cacti	Cacti	0.6.2	All	All	All
Application	Cacti	Cacti	0.6.3	All	All	All
Application	Cacti	Cacti	0.6.4	All	All	All
Application	Cacti	Cacti	0.6.5	All	All	All
Application	Cacti	Cacti	0.6.6	All	All	All
Application	Cacti	Cacti	0.6.7	All	All	All
Application	Cacti	Cacti	0.6.8	All	All	All
Application	Cacti	Cacti	0.6.8a	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	0.8.6f	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

cpe:2.3:a:cacti:cacti:0.5:-:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6:*:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6.3:*:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6.4:*:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6.5:*:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6.6:*:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6.7:*:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6.8:*:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6.8a:*:*:*:*:*:*:*:

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

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

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

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:0.8.6f:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.5:-:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6:*:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6.3:*:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6.4:*:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6.5:*:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6.6:*:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6.7:*:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6.8:*:*:*:*:*:*:*:

cpe:2.3:a:cacti:cacti:0.6.8a:*:*:*:*:*:*:*:

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:0.8.6f:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→