



CVE-2010-2545

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2010-2545
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-08-23 22:00:00 UTC
Updated	2023-02-13 03:17:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in Cacti before 0.8.7g, as used in Red Hat High Performance Computing (I

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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	0.8.7e	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
Application	Cacti	Cacti	0.8.7e	All	All	All

References						
Reference				Source	Link	
Bug 459229 – CVE-2010-2545 cacti: XSS via various object names or descriptions				CONFIRM	bugzilla.redhat.com	
CVE-2010-2545 - Red Hat Customer Portal				MISC	access.redhat.com	
svn.cacti.net/viewvc				CONFIRM	svn.cacti.net	
'Re: [oss-security] Cacti XSS fixes in 0.8.7g' - MARC				MLIST	marc.info	
Red Hat Customer Portal - Access to 24x7 support and knowledge				MISC	access.redhat.com	
svn.cacti.net/viewvc				CONFIRM	svn.cacti.net	
Cacti Cross Site Scripting and HTML Injection Vulnerabilities				BID	www.securityfocus.com	
IBM X-Force Exchange				XF	exchange.xforce.ibm	
Red Hat Customer Portal				REDHAT	rhn.redhat.com	
Cacti: The Complete RRDTool-based Graphing Solution				CONFIRM	cacti.net	

Support / Security / Advisories / / MDVSA-2010:160 Mandriva	MANDRIVA	www.mandriva.com
Red Hat High Performance Computing (HPC) Solution Multiple Vulnerabilities - Advisories - Community	SECUNIA	secunia.com
svn.cacti.net/viewvc	CONFIRM	svn.cacti.net
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
'[oss-security] Cacti XSS fixes in 0.8.7g' - MARC	MLIST	marc.info
svn.cacti.net/viewvc	CONFIRM	svn.cacti.net
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](http://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](http://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://www.mitre.org/cve). This site includes MITRE data granted under the following [license](http://www.mitre.org/cve).

Free CVE JSON API cve.report/api

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