



CVE-2008-0784

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

Summary

CVE	CVE-2008-0784
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-02-14 23:00:00 UTC
Updated	2018-10-15 22:03:00 UTC
Description	graph.php in Cacti 0.8.7 before 0.8.7b and 0.8.6 before 0.8.6k allows remote attackers to obtain the full path via an invalid l

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cacti	Cacti	0.6.7	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	0.8.6c	All	All	All
Application	Cacti	Cacti	0.8.6f	All	All	All
Application	Cacti	Cacti	0.8.6i	All	All	All
Application	Cacti	Cacti	0.8.6j	All	All	All
Application	Cacti	Cacti	0.8.7	All	All	All
Application	Cacti	Cacti	0.8.7a	All	All	All
Application	Cacti	Cacti	0.6.7	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	0.8.6c	All	All	All
Application	Cacti	Cacti	0.8.6f	All	All	All
Application	Cacti	Cacti	0.8.6i	All	All	All
Application	Cacti	Cacti	0.8.6j	All	All	All
Application	Cacti	Cacti	0.8.7	All	All	All
Application	Cacti	Cacti	0.8.7a	All	All	All

References

Reference

Support / Security / Advisories / / MDVSA-2008:052 | Mandriva

SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com

Cacti Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com

[security-announce] SUSE Security Summary Report SUSE-SR:2008:005

[SECURITY] Fedora 8 Update: cacti-0.8.7b-1.fc8

SecurityFocus

Gentoo update for cacti - Secunia Advisories - Vulnerability Information - Secunia.com

SecurityFocus

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

SecurityTracker.com Archives - Cacti Input Validation Hole Permits Cross-Site Scripting Attacks and Input Validation Flaw Lets Remote Users

Bug 432758 – cacti: multiple input saintization issues (CVE-2008-0783, CVE-2008-0784, CVE-2008-0785, CVE-2008-0786)

Cacti Multiple Input Validation Vulnerabilities

Cacti: Multiple vulnerabilities — Gentoo Linux Documentation

Cacti: The Complete RRDTool-based Graphing Solution

[SECURITY] Fedora 7 Update: cacti-0.8.7b-1.fc7

Cacti 0.8.7a Multiple Vulnerabilities - CXSecurity.com

Fedora update for cacti - Secunia Advisories - Vulnerability Intelligence - Secunia.com

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)