



CVE-2007-3477

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

Summary

CVE	CVE-2007-3477
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-06-28 18:30:00 UTC
Updated	2018-10-16 16:50:00 UTC
Description	The (a) imagearc and (b) imagefilledarc functions in GD Graphics Library (libgd) before 2.0.35 allow attackers to cause a de

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libgd	Gd Graphics Library	2.0.33	All	All	All
Application	Libgd	Gd Graphics Library	2.0.34	All	All	All
Application	Libgd	Gd Graphics Library	2.0.34	rc1	All	All
Application	Libgd	Gd Graphics Library	2.0.34	rc2	All	All
Application	Libgd	Gd Graphics Library	2.0.35	rc1	All	All
Application	Libgd	Gd Graphics Library	2.0.35	rc2	All	All
Application	Libgd	Gd Graphics Library	2.0.35	rc3	All	All
Application	Libgd	Gd Graphics Library	2.0.35	rc4	All	All
Application	Libgd	Gd Graphics Library	2.0.33	All	All	All
Application	Libgd	Gd Graphics Library	2.0.34	All	All	All
Application	Libgd	Gd Graphics Library	2.0.34	rc1	All	All
Application	Libgd	Gd Graphics Library	2.0.34	rc2	All	All
Application	Libgd	Gd Graphics Library	2.0.35	rc1	All	All
Application	Libgd	Gd Graphics Library	2.0.35	rc2	All	All
Application	Libgd	Gd Graphics Library	2.0.35	rc3	All	All
Application	Libgd	Gd Graphics Library	2.0.35	rc4	All	All
Application	Libgd	Gd Graphics Library	All	rc5	All	All

References

Reference

Slackware update for gd - Advisories - Secunia

<ftp.slackware.com/pub/slackware/slackware-11.0/patches/packages/gd-2.0.35-i486-...>

FS#74: imagefilledarc can take a lot of CPU

ReleaseNote020035 - LibGD

GD: Multiple vulnerabilities — Gentoo Linux Documentation

Gentoo update for gd - Advisories - Secunia

Fedora update for libwmf - Advisories - Community

<issues.rpath.com/browse/RPL-1643>

PTeX: Multiple vulnerabilities — Gentoo Linux Documentation

Gentoo Linux Documentation -- CTeX: Multiple vulnerabilities

Gentoo update for ptex - Advisories - Secunia

FS#92: imagearc/imagefilledarc DoS fix problem

[SECURITY] Fedora 14 Update: libwmf-0.2.8.4-27.fc14

Trustix Update for Multiple Packages - Advisories - Secunia

Fedora update for gd - Advisories - Secunia

GD Graphics Library Multiple Vulnerabilities

[SECURITY] Fedora Core 6 Update: gd-2.0.35-1.fc6

Debian update for libgd2 - Advisories - Secunia

Security Announcement

SecurityFocus

Mandriva update for tetex - Advisories - Secunia

Advisories | Mandriva

42062

rPath Update for gd and Multiple php Packages - Advisories - Secunia

Bug 277421 – CVE-2007-3472 CVE-2007-3473 CVE-2007-3474 CVE-2007-3475 CVE-2007-3476 CVE-2007-3477 CVE-2007-3478 gd variou

Advisories | Mandriva

Debian -- Security Information -- DSA-1613-1 libgd2

Fedora update for gd - Advisories - Secunia

404 Not Found

Webmail - OVH

Mandriva update for gd - Advisories - Secunia

[SECURITY] Fedora 13 Update: libwmf-0.2.8.4-22.fc13

2007-08-04

2007-0024

CVE Program record

NVD vulnerability detail

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2008-02-14	Mark J Cox	Due to the minimal impact of this flaw (temporary DoS by high CPU usage) and low likelihood of

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](#)