



# CVE-2004-0990

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2004-0990
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-03-01 05:00:00 UTC
<b>Updated</b>	2017-10-11 01:29:00 UTC
<b>Description</b>	Integer overflow in GD Graphics Library libgd 2.0.28 (libgd2), and possibly other versions, allows remote attackers to cause

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gd Graphics Library	Gdlib	1.8.4	All	All	All
Application	Gd Graphics Library	Gdlib	2.0.1	All	All	All
Application	Gd Graphics Library	Gdlib	2.0.15	All	All	All
Application	Gd Graphics Library	Gdlib	2.0.20	All	All	All
Application	Gd Graphics Library	Gdlib	2.0.21	All	All	All
Application	Gd Graphics Library	Gdlib	2.0.22	All	All	All
Application	Gd Graphics Library	Gdlib	2.0.23	All	All	All
Application	Gd Graphics Library	Gdlib	2.0.26	All	All	All
Application	Gd Graphics Library	Gdlib	2.0.27	All	All	All
Application	Gd Graphics Library	Gdlib	2.0.28	All	All	All
Application	Gd Graphics Library	Gdlib	1.8.4	All	All	All
Application	Gd Graphics Library	Gdlib	2.0.1	All	All	All
Application	Gd Graphics Library	Gdlib	2.0.15	All	All	All
Application	Gd Graphics Library	Gdlib	2.0.20	All	All	All
Application	Gd Graphics Library	Gdlib	2.0.21	All	All	All
Application	Gd Graphics Library	Gdlib	2.0.22	All	All	All
Application	Gd Graphics Library	Gdlib	2.0.23	All	All	All

Application	<a href="#">Gd Graphics Library</a>	<a href="#">Gdlib</a>	2.0.26	All	All	All
Application	<a href="#">Gd Graphics Library</a>	<a href="#">Gdlib</a>	2.0.27	All	All	All
Application	<a href="#">Gd Graphics Library</a>	<a href="#">Gdlib</a>	2.0.28	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	All	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	All	All	All	All
Application	<a href="#">Openpkg</a>	<a href="#">Openpkg</a>	2.1	All	All	All
Application	<a href="#">Openpkg</a>	<a href="#">Openpkg</a>	2.2	All	All	All
Application	<a href="#">Openpkg</a>	<a href="#">Openpkg</a>	current	All	All	All
Application	<a href="#">Openpkg</a>	<a href="#">Openpkg</a>	2.1	All	All	All
Application	<a href="#">Openpkg</a>	<a href="#">Openpkg</a>	2.2	All	All	All
Application	<a href="#">Openpkg</a>	<a href="#">Openpkg</a>	current	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.1	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.2	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.0	All	x86_64	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.1	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.2	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.1	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.2	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.0	All	x86_64	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.1	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.2	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	1.5	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.0	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.1	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.2	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	1.5	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.0	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.1	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.2	All	All	All

## References

Reference	Source	Link
SUSE Updates for Multiple Packages - Advisories - Secunia	SECUNIA	<a href="#">secunia.</a>
SuSE Security announcements: [suse-security-announce] SUSE Security Summary Report SUSE-SR:2006:003	SUSE	<a href="#">lists.sus</a>
Advisories - Mandriva Linux OS	MANDRIVA	<a href="#">www.ma</a>
Mandriva update for tetex - Advisories - Secunia	SECUNIA	<a href="#">secunia.</a>
Debian -- Security Information -- DSA-602-1 libgd2	DEBIAN	<a href="#">www.del</a>
usn/usn-25-1 - Ubuntu Linux	UBUNTU	<a href="#">www.ubi</a>
Advisories - Mandriva Linux	MANDRIVA	<a href="#">www.ma</a>
GD Graphics Library Remote Integer Overflow Vulnerability	BID	<a href="#">www.sec</a>
Repository / Oval Repository	OVAL	<a href="#">oval.cise</a>
Debian -- Security Information -- DSA-589-1 libgd1	DEBIAN	<a href="#">www.del</a>
[#RPL-939] security patch(es) for gd not included (CVE-2004-0990 CVE-2006-2906) - rPath Issue Tracking System	CONFIRM	<a href="#">issues.rp</a>
P-071: Updated "gd" Packages	CIAC	<a href="#">www.cia</a>
Debian -- Security Information -- DSA-591-1 libgd2	DEBIAN	<a href="#">www.del</a>
'libgd integer overflow' - MARC	BUGTRAQ	<a href="#">marc.inf</a>
Secunia - Advisories - Mandriva update for libwmf	SECUNIA	<a href="#">secunia.</a>
usn/usn-11-1 - Ubuntu Linux	UBUNTU	<a href="#">www.ubi</a>
rPath update for gd - Advisories - Secunia	SECUNIA	<a href="#">secunia.</a>
Support	REDHAT	<a href="#">www.rec</a>
IBM X-Force Exchange	XF	<a href="#">exchang</a>
11190	OSVDB	<a href="#">www.osv</a>
Advisories - Mandriva Linux	MANDRIVA	<a href="#">www.ma</a>
Repository / Oval Repository	OVAL	<a href="#">oval.cise</a>
Mandriva update for php - Advisories - Secunia	SECUNIA	<a href="#">secunia.</a>
2004-0058	TRUSTIX	<a href="#">www.tru</a>
Advisories - Mandriva	MANDRAKE	<a href="#">www.ma</a>
Debian -- Security Information -- DSA-601-1 libgd	DEBIAN	<a href="#">www.del</a>
CVE Program record	CVE.ORG	<a href="#">www.cve</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.</a>

No vendor comments have been submitted for this CVE.

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

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](#).

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