



# CVE-2006-3334

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

## Summary

<b>CVE</b>	CVE-2006-3334
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-06-30 23:05:00 UTC
<b>Updated</b>	2018-10-18 16:46:00 UTC
<b>Description</b>	Buffer overflow in the png_decompress_chunk function in pngutil.c in libpng before 1.2.12 allows context-dependent attack

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.0	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.1	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.10	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.2	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.3	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.4	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.5	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.6	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.7	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.7rc1	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.8	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.9	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.0	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.1	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.10	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.2	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.3	All	All	All

Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.4	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.5	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.6	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.7	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.7rc1	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.8	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	1.2.9	All	All	All
Application	<a href="#">Greg Roelofs</a>	<a href="#">Libpng</a>	All	All	All	All

## References

Reference	Source	Link
About Security Update 2008-002	CONFIRM	<a href="#">docs.</a>
Mandriva update for libpng - Advisories - Secunia	SECUNIA	<a href="#">secur</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="#">www.</a>
Gentoo Linux Documentation -- libpng: Buffer overflow	GENTOO	<a href="#">secur</a>
Secunia - Advisories - SUSE Updates for Multiple Packages	SECUNIA	<a href="#">secur</a>
Advisories - Mandriva Linux	MANDRIVA	<a href="#">www.</a>
Advisories - Mandriva Linux	MANDRIVA	<a href="#">www.</a>
Advisories - Mandriva Linux	MANDRIVA	<a href="#">www.</a>
Advisories - Mandriva Linux	MANDRIVA	<a href="#">www.</a>
Mandriva update for chromium - Advisories - Secunia	SECUNIA	<a href="#">secur</a>
Advisories - Mandriva Linux	MANDRIVA	<a href="#">www.</a>
Mandriva update for doxygen - Advisories - Secunia	SECUNIA	<a href="#">secur</a>
Security Announcement	SUSE	<a href="#">www.</a>
IBM X-Force Exchange	XF	<a href="#">exch</a>
SUSE Update for Multiple Packages - Advisories - Secunia	SECUNIA	<a href="#">secur</a>
SecurityFocus	BUGTRAQ	<a href="#">www.</a>
SourceForge.net: Files	CONFIRM	<a href="#">sourc</a>
Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	<a href="#">secur</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="#">www.</a>
Security Announcement	SUSE	<a href="#">www.</a>
Libpng Graphics Library Chunk Error Processing Buffer Overflow Vulnerability	BID	<a href="#">www.</a>
APPLE-SA-2008-03-18 Security Update 2008-002	APPLE	<a href="#">lists.a</a>
[#RPL-517] libpng vulnerable to local exploit - rPath JIRA	CONFIRM	<a href="#">issue</a>
Gentoo update for povray - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	<a href="#">secur</a>
CONFIRM - Mandriva Linux - Security - Vulnerability Intelligence - Secunia.com	GENTOO	

POV-Ray: User-assisted execution of arbitrary code — Gentoo Linux Documentation	GENTOO	<a href="#">secu...</a>
CVE Program record	CVE.ORG	<a href="#">www.</a>
NVD vulnerability detail	NVD	<a href="#">nvd.n</a>

### Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-05-14	Mark J Cox	On Red Hat Enterprise Linux 2.1, 3, 4, and 5 this is a two-byte overflow into the middle of the sta

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](#).

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