



CVE-2004-0599

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2004-0599
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-11-23 05:00:00 UTC
Updated	2017-10-11 01:29:00 UTC
Description	Multiple integer overflows in the (1) png_read_png in pngread.c or (2) png_handle_sPLT functions in pngutil.c or (3) progre

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Greg Roelofs	Libpng	All	All	All	All

References

Reference	Source	Link
Security Announcement	SUSE	www.novel
'[OpenPKG-SA-2004.035] OpenPKG Security Advisory (png)' - MARC	BUGTRAQ	marc.info
Mozilla Security Advisory	CONFIRM	www.mozil
SCOSA-2005.49	SCO	ftp.sco.com
'[FLSA-2004:2089] Updated mozilla packages fix security vulnerabilities' - MARC	FEDORA	marc.info
SCO OpenServer Release 5.0.7 Maintenance Pack 4 Released - Multiple Vulnerabilities Fixed	BID	www.secur
'UnixWare 7.1.4 : Multiple Vulnerabilities in libpng' - MARC	SCO	marc.info
Debian -- Security Information -- DSA-536-1 libpng	DEBIAN	www.debia
US-CERT Vulnerability Note VU#160448	CERT-VN	www.kb.ce
Home - Conectiva	CONNECTIVA	distro.cone
Debian -- Security Information -- DSA-571-1 libpng3	DEBIAN	www.debia
US-CERT Vulnerability Note VU#477512	CERT-VN	www.kb.ce
Advisories - Mandriva Linux	MANDRIVA	www.manc

Advisories - Mandriva Linux	MANDRIVA	www.mandriva.com
Gentoo Linux Documentation -- Mozilla, Firefox, Thunderbird, Galeon, Epiphany: New releases fix vulnerabilities	GENTOO	www.gentoo.org
Mandriva update for chromium - Advisories - Secunia	SECUNIA	secunia.com
Repository / Oval Repository	OVAL	oval.cisecurity.org
redhat.com Red Hat Support	REDHAT	www.redhat.com
FLSA:1943	FEDORA	bugzilla.fedora.org
Mandriva update for doxygen - Advisories - Secunia	SECUNIA	secunia.com
US-CERT Technical Cyber Security Alert TA04-217A -- Multiple Vulnerabilities in libpng	CERT	www.us-cert.gov
Debian -- Security Information -- DSA-570-1 libpng	DEBIAN	www.debian.org
US-CERT Vulnerability Note VU#286464	CERT-VN	www.kb.cert.gov
redhat.com Red Hat Support	REDHAT	www.redhat.com
redhat.com Red Hat Support	REDHAT	www.redhat.com
200663	SUNALERT	sunsolve.sun.com
LibPNG Graphics Library Multiple Remote Vulnerabilities	BID	www.securityfocus.com
scary.beasts.org/security/CESA-2004-001.txt	MISC	scary.beasts.org
Apple - Lists.apple.com	APPLE	lists.apple.com
Advisories - Mandriva	MANDRAKE	www.mandriva.com
Repository / Oval Repository	OVAL	oval.cisecurity.org
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
Gentoo Linux Documentation -- libpng: Numerous vulnerabilities	GENTOO	www.gentoo.org
2004-0040	TRUSTIX	www.trustix.com
'[security bulletin] SSRTSSRT4778 Rev.0 Mozilla Application Suite for HP Tru64 UNIX libpng Potential' - MARC	HP	marc.info
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 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/mitre).

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