



# CVE-2004-0396

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

## Summary

<b>CVE</b>	CVE-2004-0396
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2004-06-14 04:00:00 UTC
<b>Updated</b>	2017-10-11 01:29:00 UTC
<b>Description</b>	Heap-based buffer overflow in CVS 1.11.x up to 1.11.15, and 1.12.x up to 1.12.7, when using the pserver mechanism allow

## 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="#">Cvs</a>	<a href="#">Cvs</a>	1.11	All	All	All
Application	<a href="#">Cvs</a>	<a href="#">Cvs</a>	1.12	All	All	All
Application	<a href="#">Cvs</a>	<a href="#">Cvs</a>	1.11	All	All	All
Application	<a href="#">Cvs</a>	<a href="#">Cvs</a>	1.12	All	All	All

## References

Reference	Source	Link
Gentoo Linux Documentation -- CVS heap overflow vulnerability	GENTOO	<a href="#">security.g</a>
Secunia - Advisories - FreeBSD update for cvs	SECUNIA	<a href="#">secunia.c</a>
US-CERT Technical Cyber Security Alert TA04-147A -- CVS Heap Overflow Vulnerability	CERT	<a href="#">www.us-c</a>
Secunia - Advisories - CVS Entry Line Heap Overflow Vulnerability	SECUNIA	<a href="#">secunia.c</a>
[Full-Disclosure] SUSE Security Announcement: cvs (SuSE-SA:2004:013)	SUSE	<a href="#">lists.grok.c</a>
CVS Malformed Entry Modified and Unchanged Flag Insertion Heap Overflow Vulnerability	BID	<a href="#">www.secu</a>
Repository / Oval Repository	OVAL	<a href="#">oval.cisec</a>
US-CERT Vulnerability Note VU#192038	CERT-VN	<a href="#">www.kb.c</a>
'[FLSA-2004:1620] Updated cvs resolves security vulnerabilities' - MARC	FEDORA	<a href="#">marc.info</a>
Debian -- Security Information -- DSA-505-1 cvs	DEBIAN	<a href="#">www.debi</a>

e-matters : SECURITY	MISC	<a href="#">security.e</a>
Advisories - Mandriva	MANDRAKE	<a href="#">www.man</a>
IBM X-Force Exchange	XF	<a href="#">exchange</a>
Secunia - Advisories - Debian update for cvs	SECUNIA	<a href="#">secunia.co</a>
'cvs server buffer overflow vulnerability' - MARC	OPENBSD	<a href="#">marc.info</a>
FreeBSD-SA-04:10	FREEBSD	<a href="#">ftp.freebsd</a>
Secunia - Advisories - Red Hat update for cvs	SECUNIA	<a href="#">secunia.co</a>
Neohapsis Archives - Full Disclosure List - #0980 - [Full-Disclosure] Advisory 07/2004: CVS remote vulnerability	FULLDISC	<a href="#">archives.r</a>
Advisory 07/2004: CVS remote vulnerability	BUGTRAQ	<a href="#">cert.uni-st</a>
6305	OSVDB	<a href="#">www.osvc</a>
NetBSD-SA2004-008	NETBSD	<a href="#">ftp.NetBS</a>
Secunia - Advisories - Gentoo update for CVS	SECUNIA	<a href="#">secunia.co</a>
Repository / Oval Repository	OVAL	<a href="#">oval.cisec</a>
redhat.com   Red Hat Support	REDHAT	<a href="#">www.redh</a>
'Advisory 07/2004: CVS remote vulnerability' - MARC	BUGTRAQ	<a href="#">marc.info</a>
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE	<a href="#">www.slack</a>
O-147: Linux CVS Server Heap Overflow Vulnerability	CIAC	<a href="#">www.ciac.</a>
'[OpenPKG-SA-2004.022] OpenPKG Security Advisory (cvs)' - MARC	BUGTRAQ	<a href="#">marc.info</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.o</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.g</a>

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](#).

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