



CVE-2007-4033

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

Summary

CVE	CVE-2007-4033
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-07-27 22:30:00 UTC
Updated	2018-10-15 21:32:00 UTC
Description	Buffer overflow in the intT1_EnvGetCompletePath function in lib/t1lib/t1env.c in t1lib 5.1.1 allows context-dependent attacks

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php	Php	5.2.3	All	All	All
Application	Php	Php	5.2.3	All	All	All
Application	T1lib	T1lib	5.1.1	All	All	All
Application	T1lib	T1lib	5.1.1	All	All	All

References

Reference	Source	Link
SecurityFocus	BUGTRAQ	www.secu
T1lib intT1_Env_GetCompletePath Buffer Overflow Vulnerability	BID	www.secu
Xpdf Bugs in streams and t1lib Let Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	www.secu
Support / Security / Advisories // MDKSA-2007:189 Mandriva	MANDRIVA	www.mand
404 Not Found	FEDORA	fedoranew
Support	REDHAT	www.redh
PHP 5.2.3 - 'PHP_gd2.dll' imagepsloadfont Local Buffer Overflow (PoC) - Windows dos Exploit	EXPLOIT-DB	www.expl
Repository / Oval Repository	OVAL	oval.cisec
IBM X-Force Exchange	XF	exchange.
Support / Security / Advisories // MDKSA-2007:230 Mandriva	MANDRIVA	www.mand

PTeX: Multiple vulnerabilities — Gentoo Linux Documentation	GENTOO	security.gentoo.org
Gentoo Linux Documentation -- CTeX: Multiple vulnerabilities	GENTOO	security.gentoo.org
Gentoo update for ptex - Advisories - Secunia	SECUNIA	secunia.com
SecurityFocus	BUGTRAQ	www.securityfocus.com
[SECURITY] Fedora 7 Update: tetex-3.0-40.3.fc7	FEDORA	www.redhat.com
Gentoo Linux Documentation -- T1Lib: Buffer overflow	GENTOO	security.gentoo.org
SUSE Update for Multiple Packages - Advisories - Secunia	SECUNIA	secunia.com
SecurityFocus	BUGTRAQ	www.securityfocus.com
www.bugtraq.ir/adv/t1lib.txt	MISC	www.bugtraq.ir
Fedora update for tetex - Advisories - Secunia	SECUNIA	secunia.com
t1lib "intT1_EnvGetCompletePath()" Buffer Overflow - Advisories - Secunia	SECUNIA	secunia.com
[SECURITY] Fedora Core 6 Update: tetex-3.0-36.fc6	FEDORA	www.redhat.com
Debian update for t1lib - Advisories - Secunia	SECUNIA	secunia.com
rhn.redhat.com Red Hat Support	REDHAT	www.redhat.com
Bug 303021 – CVE-2007-4033 Buffer overflow in t1lib triggerable by long filename string	MISC	bugzilla.redhat.com
rPath update for tetex - Advisories - Secunia	SECUNIA	secunia.com
Ubuntu update for t1lib - Advisories - Secunia	SECUNIA	secunia.com
wiki.rpath.com/wiki/Advisories:rPSA-2008-0007	CONFIRM	wiki.rpath.com
SecurityFocus	BUGTRAQ	www.securityfocus.com
USN-515-1: t1lib vulnerability Ubuntu	UBUNTU	www.ubuntu.com
Mandriva update for t1lib - Advisories - Secunia	SECUNIA	secunia.com
Gentoo Bug 193437 - media-libs/t1lib <= 5.1.1 "intT1_EnvGetCompletePath()" Buffer Overflow (CVE-2007-4033)	CONFIRM	bugs.gentoo.org
Security Announcement	SUSE	www.novell.com
Mandriva update for tetex - Advisories - Secunia	SECUNIA	secunia.com
issues.rpath.com/browse/RPL-1972	CONFIRM	issues.rpath.com
Debian -- Security Information -- DSA-1390-1 t1lib	DEBIAN	www.debian.org
Support	REDHAT	www.redhat.com
Gentoo update for t1lib - Advisories - Secunia	SECUNIA	secunia.com
Red Hat update for tetex - Advisories - Secunia	SECUNIA	secunia.com
Fedora update for t1lib - Advisories - Secunia	SECUNIA	secunia.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit			
Organization	Published	Contributor	Statement

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](#)