



CVE-2014-9664

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2014-9664
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-02-08 11:59:26 UTC
Updated	2026-05-06 22:30:45 UTC
Description	FreeType before 2.5.4 does not check for the end of the data during certain parsing actions, which allows remote attackers

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

AV:N/AC:M/Au:N/C:P/I:P/A:P

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All

Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Application	Freetype	Freetype	All	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Oracle	Solaris	10.0	All	All	All
Operating System	Oracle	Solaris	11.2	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	6	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node Eus	7.1	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.6.z	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.1	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References
Reference
freetype/freetype2.git - The FreeType 2 library
Oracle Solaris Third Party Bulletin - April 2015
Mageia Advisory: MGASA-2015-0083 - Updated freetype2 packages fix security vulnerabilities
openSUSE-SU-2015:0627-1: moderate: Security update for freetype2
[SECURITY] Fedora 20 Update: freetype-2.5.0-9.fc20
freetype/freetype2.git - The FreeType 2 library
FreeType: Multiple vulnerabilities (CVE-2015-02-05) - CentOS security

FreeType: multiple vulnerabilities (GLSA 201503-05) — Gentoo security
[SECURITY] Fedora 21 Update: freetype-2.5.3-15.fc21
Support / Security / Advisories // MDVSA-2015:055 Mandriva
Debian -- Security Information -- DSA-3188-1 freetype
Red Hat Customer Portal
USN-2510-1: FreeType vulnerabilities Ubuntu
FreeType Versions Prior to 2.5.4 Multiple Remote Vulnerabilities
USN-2739-1: FreeType vulnerabilities Ubuntu
Issue 183 - google-security-research - FreeType 2.5.3 Type42 parsing out-of-bounds read in "ps_table_add" - Google Security Research - Go
CVE Program record
NVD vulnerability detail
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](#).

Free CVE JSON API [cve.report/api](#)

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