



# CVE-2014-9674

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

## Summary

<b>CVE</b>	CVE-2014-9674
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-02-08 11:59:00 UTC
<b>Updated</b>	2018-10-30 16:27:00 UTC
<b>Description</b>	The Mac_Read_POST_Resource function in base/ftobjs.c in FreeType before 2.5.4 proceeds with adding to length values v

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	10.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	15.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	10.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	15.04	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	20	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	21	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	20	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	21	All	All	All
Application	<a href="#">Freetype</a>	<a href="#">Freetype</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All

Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Solaris</a>	10.0	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Solaris</a>	11.2	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Solaris</a>	10.0	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Solaris</a>	11.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Hpc Node</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Hpc Node</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Hpc Node</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Hpc Node</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Hpc Node Eus</a>	7.1	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Hpc Node Eus</a>	7.1	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	6.6.z	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.1	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	6.6.z	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.1	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All

## References

### Reference

[SECURITY] Fedora 21 Update: freetype-2.5.3-15.fc21

[freetype/freetype2.git](#) - The FreeType 2 library

[USN-2739-1: FreeType vulnerabilities | Ubuntu](#)

[Mageia Advisory: MGASA-2015-0083 - Updated freetype2 packages fix security vulnerabilities](#)

[USN-2739-1: FreeType vulnerabilities | Ubuntu](#)

USN-2510-1: FreeType vulnerabilities | Ubuntu

FreeType: Multiple vulnerabilities (GLSA 201503-05) — Gentoo security

Support / Security / Advisories // MDVSA-2015:055 | Mandriva

[SECURITY] Fedora 20 Update: freetype-2.5.0-9.fc20

Debian -- Security Information -- DSA-3461-1 freetype

Issue 153 - google-security-research - FreeType 2.5.3 Mac font parsing heap-based buffer overflow due to multiple integer overflows - Google

Red Hat Customer Portal

openSUSE-SU-2015:0627-1: moderate: Security update for freetype2

Oracle Solaris Third Party Bulletin - April 2015

FreeType Versions Prior to 2.5.4 Multiple Remote Vulnerabilities

freetype/freetype2.git - The FreeType 2 library

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](#).

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