CVE-2014-9662

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

Summary

CVE	CVE-2014-9662
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-02-08 11:59:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	cff/cf2ft.c in FreeType before 2.5.4 does not validate the return values of point-allocation functions, which allows remote atta

Risk And Classification

Problem Types: CWE-119

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	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	Debian	Debian Linux	7.0	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	21	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	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	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-2510-1: FreeType vulnerabilities | Ubuntu
FreeType: Multiple vulnerabilities (GLSA 201503-05) — Gentoo security
Issue 185 - google-security-research - FreeType 2.5.3 CFF CharString parsing heap-based buffer overflow in "cff_builder_add_point" - Google
[SECURITY] Fedora 20 Update: freetype-2.5.0-9.fc20
openSUSE-SU-2015:0627-1: moderate: Security update for freetype2
FreeType Versions Prior to 2.5.4 Multiple Remote Vulnerabilities
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.