CVE-2014-9666

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

Summary

CVE	CVE-2014-9666
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-02-08 11:59:28 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The tt_sbit_decoder_init function in sfnt/ttsbit.c in FreeType before 2.5.4 proceeds with a count-to-size association without r

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-189 | 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
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
freetype/freetype2.git - The FreeType 2 library
[SECURITY] Fedora 20 Update: freetype-2.5.0-9.fc20
Issue 167 - google-security-research - FreeType 2.5.3 sbits parsing potential out-of-bounds read due to integer overflow - Google Security Res
FreeType: Multiple vulnerabilities (CLSA-2015:05) -- Cantoo 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
USN-2510-1: FreeType vulnerabilities | Ubuntu
FreeType Versions Prior to 2.5.4 Multiple Remote Vulnerabilities
USN-2739-1: FreeType vulnerabilities | Ubuntu
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**