CVE-2014-9665

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

Summary

CVE	CVE-2014-9665
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-02-08 11:59:27 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The Load_SBit_Png function in sfnt/pngshim.c in FreeType before 2.5.4 does not restrict the rows and pitch values of PNG

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/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	15.10	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

Vendor Declared Affected Products

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

References

Reference
openSUSE-SU-2015:0627-1: moderate: Security update for freetype2
Issue 168 - google-security-research - FreeType 2.5.3 sbix PNG handling heap-based buffer overflow due to integer overflow - Google Securit
[SECURITY] Fedora 20 Update: freetype-2.5.0-9.fc20
freetype/freetype2.git - The FreeType 2 library
FreeType: Multiple vulnerabilities (GLSA 201503-05) — Gentoo security
[SECURITY] Fedora 21 Update: freetype-2.5.3-15.fc21
freetype/freetype2.git - The FreeType 2 library
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.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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**