



CVE-2014-2240

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2014-2240
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-03-12 14:55:00 UTC
Updated	2021-01-26 12:43:00 UTC
Description	Stack-based buffer overflow in the cf2_hintmap_build function in cff/cf2hints.c in FreeType before 2.5.3 allows remote attac

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Freetype	Freetype	1.3.1	All	All	All
Application	Freetype	Freetype	2.0.0	All	All	All
Application	Freetype	Freetype	2.0.1	All	All	All
Application	Freetype	Freetype	2.0.2	All	All	All
Application	Freetype	Freetype	2.0.3	All	All	All
Application	Freetype	Freetype	2.0.4	All	All	All
Application	Freetype	Freetype	2.0.5	All	All	All
Application	Freetype	Freetype	2.0.6	All	All	All
Application	Freetype	Freetype	2.0.7	All	All	All
Application	Freetype	Freetype	2.0.8	All	All	All
Application	Freetype	Freetype	2.0.9	All	All	All
Application	Freetype	Freetype	2.1	All	All	All
Application	Freetype	Freetype	2.1.10	All	All	All
Application	Freetype	Freetype	2.1.3	All	All	All
Application	Freetype	Freetype	2.1.4	All	All	All
Application	Freetype	Freetype	2.1.5	All	All	All
Application	Freetype	Freetype	2.1.6	All	All	All

Application						
Application	Freetype	Freetype	2.1.7	All	All	All
Application	Freetype	Freetype	2.1.8	All	All	All
Application	Freetype	Freetype	2.1.8	rc1	All	All
Application	Freetype	Freetype	2.1.9	All	All	All
Application	Freetype	Freetype	2.2.0	All	All	All
Application	Freetype	Freetype	2.2.1	All	All	All
Application	Freetype	Freetype	2.3.0	All	All	All
Application	Freetype	Freetype	2.3.1	All	All	All
Application	Freetype	Freetype	2.3.10	All	All	All
Application	Freetype	Freetype	2.3.11	All	All	All
Application	Freetype	Freetype	2.3.12	All	All	All
Application	Freetype	Freetype	2.3.2	All	All	All
Application	Freetype	Freetype	2.3.3	All	All	All
Application	Freetype	Freetype	2.3.4	All	All	All
Application	Freetype	Freetype	2.3.5	All	All	All
Application	Freetype	Freetype	2.3.6	All	All	All
Application	Freetype	Freetype	2.3.7	All	All	All
Application	Freetype	Freetype	2.3.8	All	All	All
Application	Freetype	Freetype	2.3.9	All	All	All
Application	Freetype	Freetype	2.4.0	All	All	All
Application	Freetype	Freetype	2.4.1	All	All	All
Application	Freetype	Freetype	2.4.10	All	All	All
Application	Freetype	Freetype	2.4.11	All	All	All
Application	Freetype	Freetype	2.4.12	All	All	All
Application	Freetype	Freetype	2.4.2	All	All	All
Application	Freetype	Freetype	2.4.3	All	All	All
Application	Freetype	Freetype	2.4.4	All	All	All
Application	Freetype	Freetype	2.4.5	All	All	All
Application	Freetype	Freetype	2.4.6	All	All	All
Application	Freetype	Freetype	2.4.7	All	All	All
Application	Freetype	Freetype	2.4.8	All	All	All
Application	Freetype	Freetype	2.4.9	All	All	All
Application	Freetype	Freetype	2.5	All	All	All
Application	Freetype	Freetype	2.5.1	All	All	All
Application	Freetype	Freetype	1.3.1	All	All	All

Application	Freetype	Freetype	2.0.0	All	All	All
Application	Freetype	Freetype	2.0.1	All	All	All
Application	Freetype	Freetype	2.0.2	All	All	All
Application	Freetype	Freetype	2.0.3	All	All	All
Application	Freetype	Freetype	2.0.4	All	All	All
Application	Freetype	Freetype	2.0.5	All	All	All
Application	Freetype	Freetype	2.0.6	All	All	All
Application	Freetype	Freetype	2.0.7	All	All	All
Application	Freetype	Freetype	2.0.8	All	All	All
Application	Freetype	Freetype	2.0.9	All	All	All
Application	Freetype	Freetype	2.1	All	All	All
Application	Freetype	Freetype	2.1.10	All	All	All
Application	Freetype	Freetype	2.1.3	All	All	All
Application	Freetype	Freetype	2.1.4	All	All	All
Application	Freetype	Freetype	2.1.5	All	All	All
Application	Freetype	Freetype	2.1.6	All	All	All
Application	Freetype	Freetype	2.1.7	All	All	All
Application	Freetype	Freetype	2.1.8	All	All	All
Application	Freetype	Freetype	2.1.8	rc1	All	All
Application	Freetype	Freetype	2.1.9	All	All	All
Application	Freetype	Freetype	2.2.0	All	All	All
Application	Freetype	Freetype	2.2.1	All	All	All
Application	Freetype	Freetype	2.3.0	All	All	All
Application	Freetype	Freetype	2.3.1	All	All	All
Application	Freetype	Freetype	2.3.10	All	All	All
Application	Freetype	Freetype	2.3.11	All	All	All
Application	Freetype	Freetype	2.3.12	All	All	All
Application	Freetype	Freetype	2.3.2	All	All	All
Application	Freetype	Freetype	2.3.3	All	All	All
Application	Freetype	Freetype	2.3.4	All	All	All
Application	Freetype	Freetype	2.3.5	All	All	All
Application	Freetype	Freetype	2.3.6	All	All	All
Application	Freetype	Freetype	2.3.7	All	All	All
Application	Freetype	Freetype	2.3.8	All	All	All
Application	Freetype	Freetype	2.3.9	All	All	All
Application	Freetype	Freetype	2.3.9	All	All	All

Application	Freetype	Freetype	2.4.0	All	All	All
Application	Freetype	Freetype	2.4.1	All	All	All
Application	Freetype	Freetype	2.4.10	All	All	All
Application	Freetype	Freetype	2.4.11	All	All	All
Application	Freetype	Freetype	2.4.12	All	All	All
Application	Freetype	Freetype	2.4.2	All	All	All
Application	Freetype	Freetype	2.4.3	All	All	All
Application	Freetype	Freetype	2.4.4	All	All	All
Application	Freetype	Freetype	2.4.5	All	All	All
Application	Freetype	Freetype	2.4.6	All	All	All
Application	Freetype	Freetype	2.4.7	All	All	All
Application	Freetype	Freetype	2.4.8	All	All	All
Application	Freetype	Freetype	2.4.9	All	All	All
Application	Freetype	Freetype	2.5	All	All	All
Application	Freetype	Freetype	2.5.1	All	All	All
Application	Freetype	Freetype	All	All	All	All

References		
Reference	Source	Link
The FreeType Project - Browse /freetype2/2.5.3 at SourceForge.net	CONFIRM	sourceforg
USN-2148-1: FreeType vulnerabilities Ubuntu	UBUNTU	www.ubun
FreeType 'src/cff/cf2hints.c' Remote Stack Buffer Overflow Vulnerability	BID	www.secu
The FreeType Project	CONFIRM	www.freet
The FreeType Project - Bugs: bug #41697, Out-of-bounds stack-based... [Savannah]	CONFIRM	savannah.
FreeType Buffer Overflow in CFF Driver Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	www.secu
Security Advisory SA57291 - FreeType CFF Fonts Stem Hints Processing Buffer Overflow Vulnerability - Secunia	SECUNIA	secunia.cc
Security Advisory SA57447 - Ubuntu update for freetype - Secunia	SECUNIA	secunia.cc
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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