



CVE-2012-1131

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

Summary

CVE	CVE-2012-1131
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-04-25 10:10:00 UTC
Updated	2023-02-13 00:23:00 UTC
Description	FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, on 64-bit platforms allows remot

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	2.4.2	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	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	2.4.0	All	All	All
Application	Freetype	Freetype	2.4.1	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	2.4.7	All	All	All
Application	Freetype	Freetype	All	All	All	All
Application	Mozilla	Firefox Mobile	1.0	All	All	All
Application	Mozilla	Firefox Mobile	10.0	All	All	All
Application	Mozilla	Firefox Mobile	10.0.1	All	All	All
Application	Mozilla	Firefox Mobile	10.0.2	All	All	All
Application	Mozilla	Firefox Mobile	4.0	All	All	All
Application	Mozilla	Firefox Mobile	4.0	beta1	All	All
Application	Mozilla	Firefox Mobile	4.0	beta2	All	All
Application	Mozilla	Firefox Mobile	4.0	beta3	All	All
Application	Mozilla	Firefox Mobile	4.0	beta4	All	All
Application	Mozilla	Firefox Mobile	5.0	All	All	All
Application	Mozilla	Firefox Mobile	6.0	All	All	All
Application	Mozilla	Firefox Mobile	6.0.1	All	All	All
Application	Mozilla	Firefox Mobile	6.0.2	All	All	All
Application	Mozilla	Firefox Mobile	7.0	All	All	All
Application	Mozilla	Firefox Mobile	8.0	All	All	All
Application	Mozilla	Firefox Mobile	9.0	All	All	All
Application	Mozilla	Firefox Mobile	1.0	All	All	All
Application	Mozilla	Firefox Mobile	10.0	All	All	All
Application	Mozilla	Firefox Mobile	10.0.1	All	All	All
Application	Mozilla	Firefox Mobile	10.0.2	All	All	All
Application	Mozilla	Firefox Mobile	4.0	All	All	All
Application	Mozilla	Firefox Mobile	4.0	beta1	All	All
Application	Mozilla	Firefox Mobile	4.0	beta2	All	All
Application	Mozilla	Firefox Mobile	4.0	beta3	All	All
Application	Mozilla	Firefox Mobile	4.0	beta4	All	All
Application	Mozilla	Firefox Mobile	5.0	All	All	All
Application	Mozilla	Firefox Mobile	6.0	All	All	All
Application	Mozilla	Firefox Mobile	6.0.1	All	All	All
Application	Mozilla	Firefox Mobile	6.0.2	All	All	All
Application	Mozilla	Firefox Mobile	7.0	All	All	All
Application	Mozilla	Firefox Mobile	8.0	All	All	All
Application	Mozilla	Firefox Mobile	9.0	All	All	All
Application	Mozilla	Firefox Mobile	All	All	All	All

References	
Reference	Source
Bug 800589 – CVE-2012-1131 freetype: incorrect type cast allowing input sanity check bypass in ft_smooth_render_generic() (#35604)	CO
[security-announce] SUSE-SU-2012:0483-1: important: Security update for	SU:
FreeType Versions Prior to 2.4.9 Multiple Remote Vulnerabilities	BID
USN-1403-1: FreeType vulnerabilities Ubuntu	UBI
www.mandriva.com	MA
Red Hat Customer Portal	MIS
733512 – FreeType: Multiple security flaws to be fixed in v2.4.9	CO
Security Advisory SA48951 - SUSE update for freetype2 - Secunia	SEC
MFSA 2012-21: Multiple security flaws fixed in FreeType v2.4.9	CO
Security Alerts - Secunia	SEC
Security Advisory SA48508 - Ubuntu update for freetype - Secunia	SEC
About Secunia Research Flexera	SEC
oss-security - Re: CVE Request -- FreeType: Multiple security flaws to be fixed in v2.4.9	MLI
Security Alerts - Secunia	SEC
[security-announce] SUSE-SU-2012:0484-1: important: Security update for	SU:
APPLE-SA-2012-09-19-1 iOS 6	API
[security-announce] SUSE-SU-2012:0521-1: important: Security update for	SU:
Gentoo Linux Documentation -- FreeType: Multiple vulnerabilities	GE
About Secunia Research Flexera	SEC
[security-announce] openSUSE-SU-2012:0489-1: important: freetype2 update	SU:
FreeType Buffer Overflows and Memory Errors Let Remote Users Deny Service and Execute Arbitrary Code - SecurityTracker	SEC
Red Hat Customer Portal	REI
Security Advisory SA48797 - SUSE update for freetype2 - Secunia	SEC
access.redhat.com CVE-2012-1131	MIS
About the security content of iOS 6	CO
CVE Program record	CVI
NVD vulnerability detail	NVI
No vendor comments have been submitted for this CVE.	
There are currently no legacy QID mappings associated with this CVE.	

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](#).

Free CVE JSON API cve.report/api

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