



CVE-2012-1129

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

Summary

CVE	CVE-2012-1129
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-04-25 10:10:00 UTC
Updated	2021-01-26 12:43:00 UTC
Description	FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to caus

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	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 800585 – CVE-2012-1129 freetype: heap off-by-one buffer underflow in Type42 parser t42_parse_sfnts() (#35602)	CONFIRM
[security-announce] SUSE-SU-2012:0483-1: important: Security update for	SUSE
FreeType Versions Prior to 2.4.9 Multiple Remote Vulnerabilities	BID
USN-1403-1: FreeType vulnerabilities Ubuntu	UBUNTU
www.mandriva.com	MANDRIVA
733512 – FreeType: Multiple security flaws to be fixed in v2.4.9	CONFIRM
Security Advisory SA48951 - SUSE update for freetype2 - Secunia	SECUNIA
MFSA 2012-21: Multiple security flaws fixed in FreeType v2.4.9	CONFIRM
Security Alerts - Secunia	SECUNIA
Security Advisory SA48508 - Ubuntu update for freetype - Secunia	SECUNIA
About Secunia Research Flexera	SECUNIA
oss-security - Re: CVE Request -- FreeType: Multiple security flaws to be fixed in v2.4.9	MLIST
[security-announce] SUSE-SU-2012:0484-1: important: Security update for	SUSE
APPLE-SA-2012-09-19-1 iOS 6	APPLE
[security-announce] SUSE-SU-2012:0521-1: important: Security update for	SUSE
Gentoo Linux Documentation -- FreeType: Multiple vulnerabilities	GENTOO
About Secunia Research Flexera	SECUNIA
[security-announce] openSUSE-SU-2012:0489-1: important: freetype2 update	SUSE
FreeType Buffer Overflows and Memory Errors Let Remote Users Deny Service and Execute Arbitrary Code - SecurityTracker	SECTrack
Security Advisory SA48797 - SUSE update for freetype2 - Secunia	SECUNIA
About the security content of iOS 6	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
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