



CVE-2010-3855

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

Summary

CVE	CVE-2010-3855
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-11-26 20:00:00 UTC
Updated	2023-02-13 04:26:00 UTC
Description	Buffer overflow in the ft_var_readpackedpoints function in truetype/ttgxvar.c in FreeType 2.4.3 and earlier allows remote att

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	2.0.6	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	2.1.9	All	All	All
Application	Freetype	Freetype	2.2.0	All	All	All
Application	Freetype	Freetype	2.2.1	All	All	All
Application	Freetype	Freetype	2.2.10	All	All	All
Application	Freetype	Freetype	2.3.0	All	All	All
Application	Freetype	Freetype	2.3.1	All	All	All

Application						
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	1.3.1	All	All	All
Application	Freetype	Freetype	2.0.6	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	2.1.9	All	All	All
Application	Freetype	Freetype	2.2.0	All	All	All
Application	Freetype	Freetype	2.2.1	All	All	All
Application	Freetype	Freetype	2.2.10	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	All	All	All	All

--

References						
Reference						Source
APPLE-SA-2011-03-21-1 Mac OS X v10.6.7 and Security Update 2011-001						APPLE
APPLE-SA-2011-03-09-1 iOS 4.3						APPLE
Red Hat Customer Portal						MISC
FreeType 'ft_var_readpackedpoints()' Buffer Overflow Vulnerability						BID
About the security content of iOS 4.3.4 Software Update - Apple Support						CONFID
Security Advisory SA48951 - SUSE update for freetype2 - Secunia						SECUN
APPLE-SA-2011-07-15-1 iOS 4.3.4 Software Update						APPLE
Support						REDHA
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						VUPEN
Debian update for freetype - Advisories - Community						SECUN
[SECURITY] Fedora 13 Update: freetype-2.3.11-7.fc13						FEDOR
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						VUPEN
[SECURITY] Fedora 14 Update: freetype-2.4.2-4.fc14						FEDOR
USN-1013-1: FreeType vulnerabilities Ubuntu						UBUNT
freetype/freetype2.git - The FreeType 2 library						CONFID
Debian -- Security Information -- DSA-2155-1 freetype						DEBIAN
About the security content of Apple TV 4.2						CONFID
Fedora update for freetype - Secunia.com						SECUN
SecurityTracker.com Archives - FreeType Buffer Overflow in ft_var_readpackedpoints() Lets Remote Users Execute Arbitrary Code						SECTR
Red Hat update for freetype - Secunia.com						SECUN
About the security content of iOS 4.2.9 Software Update for iPhone - Apple Support						CONFID
The FreeType Project - Bugs: bug #31310, ft_var_readpackedpoints() buffer... [Savannah]						CONFID

About the security content of Mac OS X v10.6.7 and Security Update 2011-001	CONFID
About the security content of iOS 4.3	CONFID
645275 – (CVE-2010-3855) CVE-2010-3855 Freetype : Heap based buffer overflow in ft_var_readpackedpoints()	MISC
Support / Security / Advisories // MDVSA-2010:235 Mandriva	MANDR
Support / Security / Advisories // MDVSA-2010:236 Mandriva	MANDR
[SECURITY] Fedora 12 Update: freetype-2.3.11-7.fc12	FEDOR
ASA-2010-344 (RHSA-2010-0889)	CONFID
APPLE-SA-2011-07-15-2 iOS 4.2.9 Software Update for iPhone	APPLE
#602221 - freetype: CVE-2010-3855 and CVE-2010-3814 - Debian Bug report logs	CONFID
access.redhat.com CVE-2010-3855	MISC
APPLE-SA-2011-03-09-3 Apple TV 4.2	APPLE
CVE Program record	CVE.OF
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#)