



CVE-2010-3311

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

Summary

CVE	CVE-2010-3311
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-01-07 23:00:00 UTC
Updated	2023-02-13 04:23:00 UTC
Description	Integer overflow in base/ftstream.c in libXft (aka the X FreeType library) in FreeType before 2.4 allows remote attackers to c

Risk And Classification

Problem Types: CWE-189

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	2.1.8	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	2.2.10	All	All	All
Application	Freetype	Freetype	2.3.0	All	All	All

Application						
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	2.3.2	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	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	2.1.8	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	2.2.10	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	2.3.2	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	All	All	All	All

References						
Reference			Source		Link	
access.redhat.com CVE-2010-3311			MISC		acce	
Support			REDHAT		www	
Security Advisory SA48951 - SUSE update for freetype2 - Secunia			SECUNIA		secu	
access.redhat.com			REDHAT		rhn.	
USN-1013-1: FreeType vulnerabilities Ubuntu			UBUNTU		www	
Red Hat Customer Portal			MISC		acce	
Debian -- Security Information -- DSA-2116-1 freetype			DEBIAN		www	
access.redhat.com			REDHAT		rhn.	
FreeType Rendering Engine Position Value Heap Buffer Overflow Vulnerability			BID		www	
Red Hat Customer Portal			MISC		acce	
Red Hat Customer Portal			MISC		acce	
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:019			SUSE		lists	
Bug 623625 – CVE-2010-3311 freetype: Input stream position error by processing Compact Font Format (CFF) font files			CONFIRM		bug.	
Support / Security / Advisories // MDVSA-2010:201 Mandriva			MANDRIVA		www	
CVE Program record			CVE.ORG		www	
NVD vulnerability detail			NVD		nvd.	

No vendor comments have been submitted for this CVE.

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

