CVE-2010-3814

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2010-3814
State	PUBLISHED
Assigner	apple
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-11-26 20:00:02 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Heap-based buffer overflow in the Ins_SHZ function in ttinterp.c in FreeType 2.4.3 and earlier allows remote attackers to ex

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

AV:N/AC:M/Au:N/C:P/I:P/A:P

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

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	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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Sourc
FreeType TrueType Font Handling 'ttinterp.c' Remote Code Execution Vulnerability	af854a
About the security content of iOS 4.2	af854a
CVE-2010-3814	af854a
Debian update for freetype - Advisories - Community	af854a
APPLE-SA-2011-03-21-1 Mac OS X v10.6.7 and Security Update 2011-001	af854a
freetype/freetype2.git - The FreeType 2 library	af854a
Debian -- Security Information -- DSA-2155-1 freetype	af854a
APPLE-SA-2010-11-22-1 iOS 4.2	af854a
Apple iOS Multiple Vulnerabilities - Advisories - Community	af854a
USN-1013-1: FreeType vulnerabilities | Ubuntu	af854a
#602221 - freetype: CVE-2010-3855 and CVE-2010-3814 - Debian Bug report logs	af854a
About the security content of Mac OS X v10.6.7 and Security Update 2011-001	af854a
SecurityTracker.com Archives - FreeType Heap Overflow in Processing TrueType Fonts Lets Remote Users Execute Arbitrary Code	af854a
Security Advisory SA48951 - SUSE update for freetype2 - Secunia	af854a
Support / Security / Advisories / / MDVSA-2010:236 | Mandriva	af854a
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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