CVE-2009-0946

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

Summary

CVE	CVE-2009-0946
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-04-17 00:30:00 UTC
Updated	2021-04-05 19:25:00 UTC
Description	Multiple integer overflows in FreeType 2.3.9 and earlier allow remote attackers to execute arbitrary code via vectors related

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Mac Os X	10.4.11	All	All	All
Operating System	Apple	Mac Os X	10.5.8	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X Server	10.4.11	All	All	All
Operating System	Apple	Mac Os X Server	10.5.8	All	All	All
Operating System	Apple	Mac Os X Server	All	All	All	All
Application	Apple	Safari	4.0	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	8.10	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	6.0	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	2.3.3	All	All	All
Application	Freetype	Freetype	2.3.4	All	All	All
Application	Freetype	Freetype	2.3.5	All	All	All
Application	Freetype	Freetype	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	2.3.3	All	All	All
Application	Freetype	Freetype	2.3.4	All	All	All
Application	Freetype	Freetype	2.3.5	All	All	All
Application	Freetype	Freetype	All	All	All	All

Operating System	Opensuse	Opensuse	10.3	All	All	All
Operating System	Opensuse	Opensuse	11.0	All	All	All
Operating System	Opensuse	Opensuse	11.1	All	All	All
Operating System	Suse	Linux Enterprise Server	10	-	All	All
Operating System	Suse	Linux Enterprise Server	11	-	All	All

References

Reference	Source
APPLE-SA-2009-06-17-1 iPhone OS 3.0 Software Update	APPLE
freetype/freetype2.git - The FreeType 2 library	CONFIRM
APPLE-SA-2010-11-10-1 Mac OS X v10.6.5 and Security Update 2010-007	APPLE
Repository / Oval Repository	OVAL
freetype/freetype2.git - The FreeType 2 library	CONFIRM
freetype/freetype2.git - The FreeType 2 library	CONFIRM
Red Hat update for freetype - Secunia.com	SECUNIA
USN-767-1: FreeType vulnerability | Ubuntu	UBUNTU
Support	REDHAT
Debian -- Security Information -- DSA-1784-1 freetype	DEBIAN
Red Hat update for freetype - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
FreeType Multiple Vulnerabilities - Advisories - Community	SECUNIA
Debian update for freetype - Secunia.com	SECUNIA
Support	REDHAT
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:010	SUSE
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Ubuntu update for freetype - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
freetype/freetype2.git - The FreeType 2 library	CONFIRM
270268	SUNALERT
Apple Safari Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
Gentoo update for freetype - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
Gentoo Linux Documentation -- FreeType: Multiple vulnerabilities	GENTOO
About the security content of Security Update 2009-002 / Mac OS X v10.5.7	CONFIRM
US-CERT Technical Cyber Security Alert TA09-133A -- Apple Updates for Multiple Vulnerabilities	CERT
APPLE-SA-2009-06-08-1 Safari 4.0	APPLE
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Support / Security / Advisories / / MDVSA-2009:243 | Mandriva	MANDRIVA

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
504 Gateway Time-out	BID
SUSE Update for Multiple Packages - Advisories - Community	SECUNIA
About the security content of iPhone OS 3.0 Software Update	CONFIRM
About the security content of Safari 4.0	CONFIRM
APPLE-SA-2009-05-12 Security Update 2009-002 / Mac OS X v10.5.7	APPLE
Support	REDHAT
Red Hat update for freetype - Secunia.com	SECUNIA
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
491384 – (CVE-2009-0946) CVE-2009-0946 freetype: multiple integer overflows	CONFIRM
About the security content of Mac OS X v10.6.5 and Security Update 2010-007	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.

© 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 registred 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**