



CVE-2008-1808

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

Summary

CVE	CVE-2008-1808
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-06-16 19:41:00 UTC
Updated	2021-01-26 12:41:00 UTC
Description	Multiple off-by-one errors in FreeType2 before 2.3.6 allow context-dependent attackers to execute arbitrary code via (1) a 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	2.1.10	All	All	All
Application	Freetype	Freetype	2.1.7	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	2.1.10	All	All	All
Application	Freetype	Freetype	2.1.7	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

References

Reference

About the security content of iPhone v2.1

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Repository / Oval Repository

VMware Workstation 6 Release Notes

APPLE-SA-2009-02-12 Security Update 2009-001

VMware Player Release Notes

FreeType TrueType Font 'SHC' Heap Buffer Overflow Vulnerability

rPath update for freetype - Secunia.com

Webmail - OVH

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Gentoo Linux Documentation -- VMware Player, Server, Workstation: Multiple vulnerabilities

SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com

FreeType: User-assisted execution of arbitrary code — Gentoo Linux Documentation

VMware Server Release Notes

Red Hat update for freetype - Secunia Advisories - Vulnerability Information - Secunia.com

FreeType Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Fedora update for freetype - Secunia Advisories - Vulnerability Intelligence - Secunia.com

[Full-disclosure] VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address in

FreeType Printer Font Binary Heap Buffer Overflow Vulnerability

SecurityFocus

APPLE-SA-2008-09-12 iPhone v2.1

Support

VMware ESX Server Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Support

Support

FreeType 2.3.5-20130522-1 Debian 7.0.0-1 Ubuntu 12.04 LTS 12.04 LTS 12.04 LTS

FreeType2 Heap Overflows in Parsing PFB and TTF Font Files Lets Remote Users Execute Arbitrary Code - Security Tracker
239006
Webmail - OVH
APPLE-SA-2008-09-09 iPod touch v2.1
Webmail - OVH
Gentoo update for freetype - Secunia Advisories - Vulnerability Intelligence - Secunia.com
SourceForge.net: The FreeType Project: Files
Sun Solaris FreeType Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com
VMSA-2008-0014.3 - VMware
About the security content of iPod touch v2.1
Webmail - OVH
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com
VMware Workstation 5.5 Release Notes
USN-643-1: FreeType vulnerabilities Ubuntu
Red Hat update for freetype - Secunia Advisories - Vulnerability Intelligence - Secunia.com
wiki.rpath.com/wiki/Advisories:rPSA-2008-0255
VMware Player Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Apple iPod Touch Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com
VMware Player Release Notes
[SECURITY] Fedora 8 Update: freetype-2.3.5-4.fc8
ASA-2008-318 (RHSA-2008-0556)
Apple iPhone Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com
VMware Fusion Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com
issues.rpath.com/browse/RPL-2608
Avaya Communication Manager FreeType Multiple Vulnerabilities - Advisories - Secunia
Red Hat update for freetype - Secunia Advisories - Vulnerability Intelligence - Secunia.com
[security-announce] SUSE Security Summary Report SUSE-SR:2008:014
Support / Security / Advisories // MDVSA-2008:121 Mandriva
VMware Workstation Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com
[SECURITY] Fedora 9 Update: freetype-2.3.5-6.fc9
SecurityFocus
About the security content of Security Update 2009-001
Ubuntu update for freetype - Secunia Advisories - Vulnerability Intelligence - Secunia.com
20080610 Multiple Vendor FreeType2 Multiple Heap Overflow Vulnerabilities
CVE Program record
NVD vulnerability detail

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](#)