



CVE-2006-0747

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2006-0747 |
| State | PUBLISHED |
| Assigner | redhat |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2006-05-23 10:06:00 UTC |
| Updated | 2025-04-03 01:03:51 UTC |
| Description | Integer underflow in Freetype before 2.2 allows remote attackers to cause a denial of service (crash) via a font file with an c |

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

EPSS: 0.459330000 probability, percentile 0.976380000 (date 2026-04-20)

Problem Types: CWE-189 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------|--------|---------|---------|--------|---------|----------|
|------|--------|---------|---------|--------|---------|----------|

| 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 | Source | | | | | |
| #102705: Security Vulnerabilities (Integer Overflows and a Denial of Service) in the FreeType 2 Font Engine | af854a3a-212 | | | | | |
| SUSE update for freetype2 - Advisories - Secunia | af854a3a-212 | | | | | |
| APPLE-SA-2009-05-12 Security Update 2009-002 / Mac OS X v10.5.7 | af854a3a-212 | | | | | |
| Mandriva update for freetype2 - Advisories - Secunia | af854a3a-212 | | | | | |
| About the security content of Security Update 2009-002 / Mac OS X v10.5.7 | af854a3a-212 | | | | | |
| SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: freetype2 (SUSE-SA:2006:037) | af854a3a-212 | | | | | |
| patches.sgi.com/support/free/security/advisories/20060701-01-U | af854a3a-212 | | | | | |
| Repository / Oval Repository | af854a3a-212 | | | | | |
| USN-291-1: FreeType vulnerabilities Ubuntu security notices | af854a3a-212 | | | | | |
| Support | af854a3a-212 | | | | | |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | af854a3a-212 | | | | | |
| Secunia - Advisories - Ubuntu update for libfreetype6 | af854a3a-212 | | | | | |
| Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com | af854a3a-212 | | | | | |
| Sun Solaris FreeType Integer Overflow and Underflow Vulnerabilities - Advisories - Secunia | af854a3a-212 | | | | | |
| FreeType TTF File Remote Buffer Overflow Vulnerability | af854a3a-212 | | | | | |
| Webmail - OVH | af854a3a-212 | | | | | |
| Advisories - Mandriva Linux | af854a3a-212 | | | | | |
| Red Hat update for freetype - Advisories - Secunia | af854a3a-212 | | | | | |
| Debian -- Security Information -- DSA-1095-1 freetype | af854a3a-212 | | | | | |
| SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia | af854a3a-212 | | | | | |
| SecurityFocus | af854a3a-212 | | | | | |
| [#RPL-429] CVE-2006-0747 CVE-2006-1861 CVE-2006-2661 multiple freetype vulnerabilities - rPath JIRA | af854a3a-212 | | | | | |
| ASA-2006-176 (RHSA-2006-0500) | af854a3a-212 | | | | | |
| Secunia - Advisories - rPath update for freetype | af854a3a-212 | | | | | |
| 183676 – CVE-2006-0747 Freetype integer underflow (CVE-2006-2661) | af854a3a-212 | | | | | |
| SecurityTracker.com Archives - FreeType Integer Overflows Let Remote Users Execute Arbitrary Code | af854a3a-212 | | | | | |
| Debian update for freetype - Advisories - Secunia | af854a3a-212 | | | | | |
| US-CERT Technical Cyber Security Alert TA09-133A -- Apple Updates for Multiple Vulnerabilities | af854a3a-212 | | | | | |

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 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](#)