# CVE-2010-2805

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2010-2805 |
| **State** | PUBLISHED |
| **Assigner** | redhat |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2010-08-19 18:00:04 UTC |
| **Updated** | 2026-04-29 01:13:23 UTC |
| **Description** | The FT_Stream_EnterFrame function in base/ftstream.c in FreeType before 2.4.2 does not properly validate certain positio |

## 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-20 | 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 |
|---|---|---|---|---|---|---|
| Operating System | Apple | Iphone Os | All | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Apple | Mac Os X | All | All | All | All |
| Operating System | Apple | Tvos | All | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 10.04 | 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 | 9.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 9.10 | 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 | Source |
|---|---|
| 'Re: [oss-security] CVE Request -- FreeType -- Memory corruption' - MARC | af854a3a-2127-422b-91ae-364da266 |
| About the security content of Mac OS X v10.6.5 and Security Update 2010-007 | af854a3a-2127-422b-91ae-364da266 |
| APPLE-SA-2010-11-10-1 Mac OS X v10.6.5 and Security Update 2010-007 | af854a3a-2127-422b-91ae-364da266 |
| About the security content of iOS 4.2 | af854a3a-2127-422b-91ae-364da266 |
| The FreeType Project - Bugs: bug #30644, Bad CFF font file causes crash [Savannah] | af854a3a-2127-422b-91ae-364da266 |
| USN-972-1: FreeType vulnerabilities \| Ubuntu | af854a3a-2127-422b-91ae-364da266 |
| The FreeType Project | af854a3a-2127-422b-91ae-364da266 |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | af854a3a-2127-422b-91ae-364da266 |
| Browse The FreeType Project Files on SourceForge.net | af854a3a-2127-422b-91ae-364da266 |
| Ubuntu update for freetype - Advisories - Community | af854a3a-2127-422b-91ae-364da266 |
| FreeType Multiple Vulnerabilities - Advisories - Community | af854a3a-2127-422b-91ae-364da266 |
| Bug #617019 “FreeType security fixes in 2.4.2” : Maverick (10.10) : Bugs : freetype package : Ubuntu | af854a3a-2127-422b-91ae-364da266 |
| APPLE-SA-2010-11-22-1 iOS 4.2 | af854a3a-2127-422b-91ae-364da266 |
| Support | af854a3a-2127-422b-91ae-364da266 |
| Apple iOS Multiple Vulnerabilities - Advisories - Community | af854a3a-2127-422b-91ae-364da266 |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | af854a3a-2127-422b-91ae-364da266 |
| About the security content of Apple TV software update 4.1 | af854a3a-2127-422b-91ae-364da266 |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | af854a3a-2127-422b-91ae-364da266 |
| Security Advisory SA48951 - SUSE update for freetype2 - Secunia | af854a3a-2127-422b-91ae-364da266 |
| Apple TV Multiple Vulnerabilities - Advisories - Community | af854a3a-2127-422b-91ae-364da266 |
| freetype/freetype2.git - The FreeType 2 library | af854a3a-2127-422b-91ae-364da266 |
| Malformed Request | af854a3a-2127-422b-91ae-364da266 |

| | |
|---|---|
| Malformed Request | af854a3a-2127-422b-91ae-364da266 |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | af854a3a-2127-422b-91ae-364da266 |
| 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.