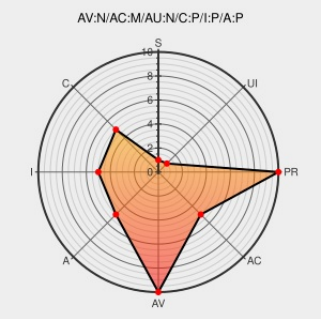
CVE-2010-2499

Published on: 08/19/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 03:06:56 AM UTC

CVE-2010-2499

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Mac Os X from Apple contain the following vulnerability:

Buffer overflow in the Mac_Read_POST_Resource function in base/ftobjs.c in FreeType before 2.4.0 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted LaserWriter PS font file with an embedded PFB fragment.

CVE-2010-2499 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[ft] FreeType 2.4.0 has been released	Patch, lists.nongnu.org, text/html	MLIST [freetype] 20100712 FreeType 2.4.0 has been released
Support / Security / Advisories / / MDVSA-2010:137 | Mandriva	www.mandriva.com, text/html	MANDRIVA MDVSA-2010:137
'[oss-security] Multiple bugs in freetype' - MARC	marc.info, text/html	MLIST [oss-security] 20100713 Multiple bugs in freetype
APPLE-SA-2010-11-10-1 Mac OS X v10.6.5 and Security Update 2010-007	lists.apple.com, text/html	APPLE APPLE-SA-2010-11-10-1
freetype/freetype2.git - The FreeType 2 library	git.savannah.gnu.org, text/html	CONFIRM git.savannah.gnu.org/cgit/freetype/freetype2.git/commit/?

		id=c69891a1345640096fbf396e8dd567fe879ce233
Security Advisory SA48951 - SUSE update for freetype2 - Secunia	web.archive.org text/html	SECUNIA 48951
SecurityTracker.com Archives - FreeType 2 Font File Processing Errors Let Remote Users Execute Arbitrary Code	securitytracker.com text/html	SECTRACK 1024266
Debian -- Security Information -- DSA-2070-1 freetype	www.debian.org Depreciated Link text/html	DEBIAN DSA-2070
The FreeType Project - Bugs: bug #30248, SIGSEGV - write to non-mapped... [Savannah]	savannah.nongnu.org text/xml	CONFIRM savannah.nongnu.org/bugs/?30248
The FreeType Project - Bugs: bug #30249, Heap corruption in base/* (Mac... [Savannah]	savannah.nongnu.org text/xml	CONFIRM savannah.nongnu.org/bugs/?30249
Support	www.redhat.com text/html	REDHAT RHSA-2010:0578
USN-963-1: FreeType vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-963-1
Bug 613162 – CVE-2010-2499 freetype: buffer overflow vulnerability	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=613162
freetype/freetype2.git - The FreeType 2 library	git.savannah.gnu.org text/html	CONFIRM git.savannah.gnu.org/cgit/freetype/freetype2.git/commit/?id=f29f741efbba0a5ce2f16464f648fb8d026ed4c8
'Re: [oss-security] Multiple bugs in freetype' - MARC	marc.info text/html	MLIST [oss-security] 20100714 Re: Multiple bugs in freetype
About the security content of Mac OS X v10.6.5 and Security Update 2010-007	web.archive.org text/html Inactive Link Not Archived	CONFIRM support.apple.com/kb/HT4435

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	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
Operating System	Debian	Debian Linux	5.0	All	All	All
Application	Freetype	Freetype	All	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	2.3.0	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	2.3.2	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	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	2.3.0	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	2.3.2	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	All	All	All	All

cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:6.06:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:8.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.10:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:*:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.0.9:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.1:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.1.10:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.1.6:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.1.7:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.1.8:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.1.9:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.2.10:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.10:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.11:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.7:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.8:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.9:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.0.9:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.1:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.1.10:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.1.6:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.1.7:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.1.8:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.1.9:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.2.10:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.10:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.11:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.7:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.8:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.3.9:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report