

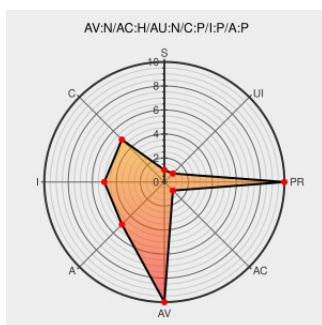


CVE-2010-2520

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

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

CVE-2010-2520

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Mac Os X](#) from [Apple](#) contain the following vulnerability:

Heap-based buffer overflow in the `Ins_IUP` function in `truetype/ttinterp.c` in FreeType before 2.4.0, when TrueType bytecode support is enabled, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted font file.

CVE-2010-2520 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5.1 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

HIGH

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

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](#)

Security Advisory SA48951 - SUSE update for
freetype2 - Secunia

[web.archive.org](#)
[text/html](#)

[SECUNIA 48951](#)

Debian -- Security Information -- DSA-2070-1 freetype	www.debian.org Deprecated Link text/html	DEBIAN DSA-2070
The FreeType Project - Bugs: bug #30361, Possible heap corruption [Savannah]	savannah.nongnu.org text/xml	CONFIRM savannah.nongnu.org/bugs/?30361
freetype/freetype2.git - The FreeType 2 library	git.savannah.gnu.org text/html	CONFIRM git.savannah.gnu.org/cgiit/freetype/freetype2.git/commit/?id=888cd1843e935fe675cf2ac303116d4ed5b9d54b
USN-963-1: FreeType vulnerabilities Ubuntu	www.ubuntu.com text/html	UBUNTU USN-963-1
Bug 613198 – CVE-2010-2520 freetype: heap buffer overflow vulnerability in truetype bytecode support	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=613198
'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

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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 →](#)