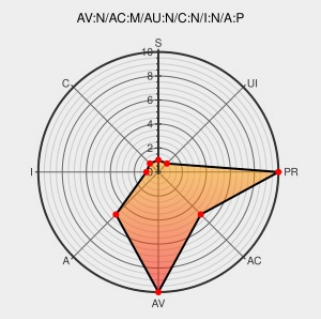
CVE-2010-3053

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

Last Modified on: 03/23/2021 11:23:02 PM UTC

CVE-2010-3053

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



Certain versions of Freetype from Freetype contain the following vulnerability:

bdf/bdflib.c in FreeType before 2.4.2 allows remote attackers to cause a denial of service (application crash) via a crafted BDF font file, related to an attempted modification of a value in a static string.

CVE-2010-3053 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
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
Apple iOS Multiple Vulnerabilities - Advisories - Community	web.archive.org text/html	SECUNIA 42314
About the security content of Apple TV software update 4.1	support.apple.com text/html	CONFIRM support.apple.com/kb/HT4457
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2010-3045
Apple TV Multiple Vulnerabilities - Advisories - Community	web.archive.org text/html	SECUNIA 42317

[security-announce] SUSE Security Summary Report: SUSE-SR:2010:019	lists.opensuse.org text/html	SUSE SUSE-SR:2010:019
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2010-3046
About the security content of iOS 4.2	support.apple.com text/html	CONFIRM support.apple.com/kb/HT4456
Bug #617019 “FreeType security fixes in 2.4.2” : Maverick (10.10) : Bugs : freetype package : Ubuntu	bugs.launchpad.net text/html	CONFIRM bugs.launchpad.net/ubuntu/maverick/+source/freetype/+bug/617019
APPLE-SA-2010-11-22-1 iOS 4.2	lists.apple.com text/html	APPLE APPLE-SA-2010-11-22-1
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
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	2.3.12	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	2.4.0	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	2.3.12	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	2.4.0	All	All	All
Application	Freetype	Freetype	All	All	All	All

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:2.3.12:*:*:*:*:*:*:*:

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:2.4.0:*:*:*:*:*:*:*:

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:2.3.12:*:*:*:*:*:*:*:

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:2.4.0:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→