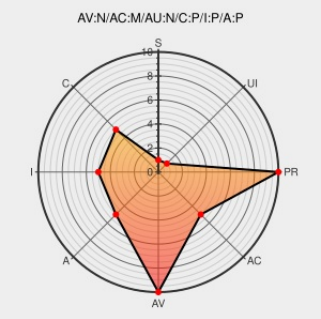
CVE-2014-2241

Published on: 03/18/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:59 PM UTC

CVE-2014-2241

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

The (1) cf2_initLocalRegionBuffer and (2) cf2_initGlobalRegionBuffer functions in cff/cf2ft.c in FreeType before 2.5.3 do not properly check if a subroutine exists, which allows remote attackers to cause a denial of service (assertion failure), as demonstrated by a crafted ttf file.

CVE-2014-2241 has been assigned by cve@mitre.org 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
USN-2148-1: FreeType vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2148-1
The FreeType Project - Bugs: bug #41697, Out-of-bounds stack-based... [Savannah]	savannah.nongnu.org text/xml	CONFIRM savannah.nongnu.org/bugs/?41697
oss-security - Re: Two stack-based issues in freetype [NOT a request]	www.openwall.com text/html	MLIST [oss-security] 20140312 Re: Two stack-based issues in freetype [NOT a request]
freetype/freetype2.git - The FreeType 2 library	Exploit Patch git.savannah.gnu.org text/html	CONFIRM git.savannah.gnu.org/cgit/freetype/freetype2.git/commit/?id=135c3faebb96f8f550bd4f318716f2e1e095a969
Security Advisory SA57447 - Ubuntu update for freetype - Secunia	web.archive.org text/html	SECUNIA 57447

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	Canonical	Ubuntu Linux	13.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Application	Freetype	Freetype	2.5	All	All	All
Application	Freetype	Freetype	2.5.1	All	All	All
Application	Freetype	Freetype	2.5	All	All	All
Application	Freetype	Freetype	2.5.1	All	All	All
Application	Freetype	Freetype	All	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:13.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:13.10:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.5:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.5:*:*:*:*:*:*:*:

cpe:2.3:a:freetype:freetype:2.5.1:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→