



CVE-2017-8374

Published on: 04/30/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:43 PM UTC

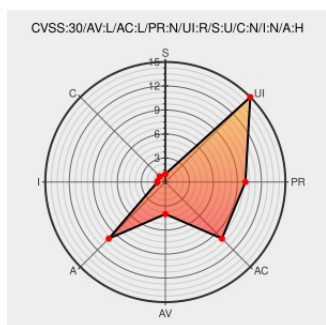
CVE-2017-8374

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Mad Libmad](#) from [Underbit](#) contain the following vulnerability:

The `mad_bit_skip` function in `bit.c` in Underbit MAD libmad 0.15.1b allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted audio file.

CVE-2017-8374 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

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
Debian -- Security Information -- DSA-4192-1 libmad	www.debian.org Deprecated Link text/html	DEBIAN DSA-4192
libmad: heap-based buffer overflow in mad_bit_skip	Exploit	MISC blogs.gentoo.org/ago/2017/04/30/libmad-heap-based-

(bit.c) | agostino's blog

Third Party Advisory

VDB Entry

blogs.gentoo.org

text/html

buffer-overflow-in-mad_bit_skip-bit-c/

[SECURITY] [DLA 1380-1] libmad security update

lists.debian.org

text/html

MLIST [debian-lts-announce] 20180518 [SECURITY] [DLA 1380-1] libmad security update

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.

Related QID Numbers

501040 Alpine Linux Security Update for libmad

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Underbit	Mad Libmad	0.15.1b	All	All	All
Application	Underbit	Mad Libmad	0.15.1b	All	All	All

cpe:2.3:a:underbit:mad_libmad:0.15.1b:****:***:

cpe:2.3:a:underbit:mad_libmad:0.15.1b:****:***:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →