



CVE-2018-7263

Published on: 02/20/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:39 PM UTC

CVE-2018-7263

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



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

The `mad_decoder_run()` function in `decoder.c` in Underbit libmad through 0.15.1b allows remote attackers to cause a denial of service (SIGABRT because of double free or corruption) or possibly have unspecified other impact via a crafted file. NOTE: this may overlap CVE-2017-11552.

CVE-2018-7263 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector

Attack Complexity

Privileges Required

User Interaction

NETWORK

LOW

NONE

NONE

Scope

Confidentiality Impact

Integrity Impact

Availability Impact

UNCHANGED

HIGH

HIGH

HIGH

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

Bug 1081784 – VUL-1: libmad: double free or corruption

[Issue Tracking](#)

[Third Party Advisory](#)

[bugzilla.suse.com](#)

[MISC bugzilla.suse.com/show_bug.cgi?id=1081784](https://bugzilla.suse.com/show_bug.cgi?id=1081784)

[text/html](#)

#870608 - CVE-2017-11548 - Debian Bug report logs

[Mailing List](#)[Third Party Advisory](#)[bugs.debian.org](#)[text/html](#)[@ MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=870608](#)

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[901200](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libmad (7264)[940328](#) AlmaLinux Security Update for GStreamer, (ALSA-2020:1631)[960244](#) Rocky Linux Security Update for GStreamer, (RLSA-2020:1631)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Underbit	Libmad	All	All	All	All
cpe:2.3:a:underbit:libmad:*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)