

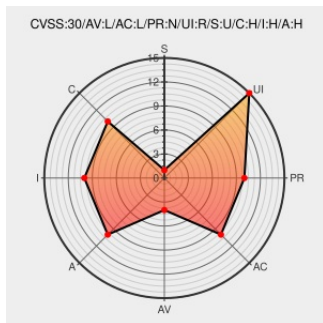


CVE-2017-11311

Published on: 07/13/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:24 PM UTC

CVE-2017-11311

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

Certain versions of [Libopenmpt](#) from [Openmpt](#) contain the following vulnerability:

soundlib/Load_psm.cpp in OpenMPT through 1.26.12.00 and libopenmpt before 0.2.8461-beta26 has a heap buffer overflow with the potential for arbitrary code execution via a crafted PSM File that triggers use of the same sample slot for two samples.

CVE-2017-11311 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
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
WebSVN - openmpt - Rev 8438 - /branches/OpenMPT-1.26/	Issue Tracking Patch Third Party Advisory source.openmpt.org text/html	CONFIRM source.openmpt.org/browse/openmpt/branches/OpenMPT-1.26/?op=revision&rev=8438

WebSVN – openmpt – /trunk/ – Rev 6800

Issue Tracking

Patch

Third Party Advisory

source.openmpt.org

text/html

CONFIRM

source.openmpt.org/browse/openmpt/trunk/?rev=6800

libopenmpt and openmpt123 - libopenmpt security updates 0.2.8461-beta26, 0.2.7561-beta20.5-p7, 0.2.7386-beta20.3-p10

Patch

Vendor Advisory

lib.openmpt.org

text/html

CONFIRM

lib.openmpt.org/libopenmpt/md_announce-2017-07-07.html

#867579 - libopenmpt: CVE-2017-11311 - Debian Bug report logs

Issue Tracking

Patch

Third Party Advisory

bugs.debian.org

text/html

CONFIRM

bugs.debian.org/867579

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
Application	Openmpt	Libopenmpt	All	beta25	All	All
Application	Openmpt	Openmpt	All	All	All	All

cpe:2.3:a:openmpt:libopenmpt*:beta25:*.***.***:

cpe:2.3:a:openmpt:openmpt:*.***.***.***:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→