



CVE-2019-17113

Published on: 10/03/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:37 PM UTC

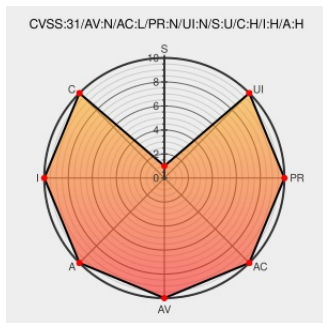
CVE-2019-17113

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

In libopenmpt before 0.3.19 and 0.4.x before 0.4.9, ModPlug_InstrumentName and ModPlug_SampleName in libopenmpt_modplug.c do not restrict the lengths of libmodplug output-buffer strings in the C API, leading to a buffer overflow.

CVE-2019-17113 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: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-4729-1 libopenmpt	www.debian.org Deprecated Link text/html	DEBIAN DSA-4729
[security-announce]	lists.opensuse.org	SUSE openSUSE-SU-2019:2306

openSUSE-SU-2019:2306-1: important: Security update	text/html	
Comparing libopenmpt-0.4.8...libopenmpt-0.4.9 · OpenMPT/openmpt · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/OpenMPT/openmpt/compare/libopenmpt-0.4.8...libopenmpt-0.4.9
[SECURITY] [DLA 2308-1] libopenmpt security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20200801 [SECURITY] [DLA 2308-1] libopenmpt security update
WebSVN – openmpt – /trunk/OpenMPT/ – Rev 12127	Patch Third Party Advisory source.openmpt.org text/html	MISC source.openmpt.org/browse/openmpt/trunk/OpenMPT/?op=revision&rev=12127&peg=12127
[Fix] libmodplug: C API: Limit the length of strings copied to the ou... · OpenMPT/openmpt@927688d · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/OpenMPT/openmpt/commit/927688ddab43c2b203569de79407a899e734fa
Comparing libopenmpt-0.3.18...libopenmpt-0.3.19 · OpenMPT/openmpt · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/OpenMPT/openmpt/compare/libopenmpt-0.3.18...libopenmpt-0.3.19
[security-announce] openSUSE-SU-2019:2319-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2019:2319

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	All	All	All
Application	Openmpt	Libopenmpt	All	All	All	All
cpe:2.3:a:openmpt:libopenmpt:*****:						
cpe:2.3:a:openmpt:libopenmpt:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)