



CVE-2019-20016

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2019-20016
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-27 02:15:00 UTC
Updated	2020-01-08 21:22:00 UTC
Description	libmysofa before 2019-11-24 does not properly restrict recursive function calls, as demonstrated by reports of stack consum

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Symonics	Libmysofa	All	All	All	All
Application	Symonics	Libmysofa	All	All	All	All

References

Reference

Fixed recursive function calls · hoene/libmysofa@2e6fac6 · GitHub

There is a stack-based buffer overflow in the readOHDRHeaderMessageDatatype function of dataobject.c(at 216) · Issue #84 · hoene/libmyso

There is a stack-based buffer overflow in the directblockRead function of fractalhead.c(at 172) · Issue #83 · hoene/libmysofa · GitHub

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[750304](#) OpenSUSE Security Update for libmysofa (openSUSE-SU-2021:0444-1)

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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