



CVE-2021-3756

Published on: 10/29/2021 12:00:00 AM UTC

Last Modified on: 12/22/2021 05:37:00 PM UTC

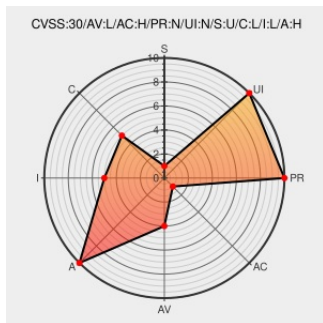
CVE-2021-3756 - advisory for 7ca8d9ea-e2a6-4294-af28-70260bb53bc1

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Fedora](#) from [Fedoraproject](#) contain the following vulnerability:

libmysofa is vulnerable to Heap-based Buffer Overflow

CVE-2021-3756 has been assigned by security@huntr.dev to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **hoene** - **hoene/libmysofa** version < 1.2.1

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
huntr: Disclose & Fix Security Vulnerabilities in Open Source	huntr.dev text/html Inactive Link Not Archived	CONFIRM huntr.dev/bounties/7ca8d9ea-e2a6-4294-af28-70260bb53bc1

Open Source

Fix for issue 163 ·
hoene/libmysofa@890400e
· GitHub

[github.com](#)
[text/html](#)

MISC
[github.com/hoene/libmysofa/commit/890400ebd092c574707d0c132124f8ff047e20c](#)

[SECURITY] Fedora 34
Update: libmysofa-1.2.1-
1.fc34 - package-announce
- Fedora Mailing-Lists

[lists.fedoraproject.org](#)
[text/html](#)

FEDORA FEDORA-2021-28b495e9e0

[SECURITY] Fedora 35
Update: libmysofa-1.2.1-
1.fc35 - package-announce
- Fedora Mailing-Lists

[lists.fedoraproject.org](#)
[text/html](#)

FEDORA FEDORA-2021-36ac17e5ac

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

184133 Debian Security Update for libmysofa (CVE-2021-3756)

282115 Fedora Security Update for libmysofa (FEDORA-2021-28b495e9e0)

282116 Fedora Security Update for libmysofa (FEDORA-2021-36ac17e5ac)

690795 Free Berkeley Software Distribution (FreeBSD) Security Update for libmysoft (4d763c65-9246-11ec-9aa3-4ccc6adda413)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Symonics	Libmysofa	All	All	All	All
cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:						
cpe:2.3:a:symonics:libmysofa:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
@CVEreport	CVE-2021-3756 : libmysofa is vulnerable to Heap-based Buffer Overflow... cve.report/CVE-2021-3756	2021-10-29 15:59:06
@threatmeter	CVE-2021-3756 libmysofa is vulnerable to Heap-based Buffer Overflow (CVSS:0.0) (Last Update:2021-10-29) ift.tt/3w25IM2	2021-10-30 07:09:57

© [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](#)