



# LibreChat's IDOR in SSE Stream Subscription Allows Reading Other Users' Chats

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

## Summary

<b>CVE</b>	CVE-2026-31950
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-27 20:16:30 UTC
<b>Updated</b>	2026-03-30 20:32:16 UTC
<b>Description</b>	LibreChat is a ChatGPT clone with additional features. In versions 0.8.2-rc2 through 0.8.2-rc3, the SSE streaming endpoint

## Risk And Classification

**Primary CVSS:** v3.1 5.3 MEDIUM from security-advisories@github.com

**CVSS:** 3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

**EPSS:** 0.000300000 probability, percentile 0.084270000 (date 2026-04-01)

**Problem Types:** CWE-284 | CWE-639 | CWE-284 CWE-284: Improper Access Control

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

#### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Librechat	Librechat	0.8.2	rc2	All	All
Application	Librechat	Librechat	0.8.2	rc3	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Danny-avila	LibreChat	affected >= 0.8.2-rc2, < 0.8.2	Not specified

#### References

Reference	Source	Link	Tags
github.com/danny-avila/LibreChat/security/advisories/GHSA-f6rf-vm44-wh5g	security-advisories@github.com	github.com	Exploit, Vendor
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© 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.

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)