



LoLLMs WEBUI has unauthenticated Server-Side Request Forgery (SSRF) in /api/proxy endpoint

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

Summary

CVE	CVE-2026-33340
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-24 17:16:44 UTC
Updated	2026-04-20 20:22:05 UTC
Description	LoLLMs WEBUI provides the Web user interface for Lord of Large Language and Multi modal Systems. A critical Server-Side Request Forgery (SSRF) vulnerability was discovered in the /api/proxy endpoint, allowing an attacker to bypass authentication and perform arbitrary requests to internal systems.

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from security-advisories@github.com

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

EPSS: 0.162630000 probability, percentile 0.948380000 (date 2026-04-20)

Problem Types: CWE-306 | CWE-918 | CWE-306 CWE-306: Missing Authentication for Critical Function | CWE-918 CWE-918: Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
3.1	CNA	DECLARED	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lollms	Lollms Web Ui	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	ParisNeo	Lollms-webui	affected <= 8c5dcef63d847bb3d027ec74915d8fe4afd3014e	Not specified

References

Reference	Source	Link
github.com/ParisNeo/lollms-webui/security/advisories/GHSA-mcwr-5469-pxj4	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
github.com/ParisNeo/lollms-webui/blob/8c5dcef63d847bb3d027ec74915d8fe4af...	security-advisories@github.com	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report