



# Insecure Direct Object Reference (IDOR) in parisneo/lollms

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

## Summary

<b>CVE</b>	CVE-2026-0562
<b>State</b>	PUBLISHED
<b>Assigner</b>	@huntr_ai
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-29 18:16:14 UTC
<b>Updated</b>	2026-03-31 19:30:04 UTC
<b>Description</b>	A critical security vulnerability in parisneo/lollms versions up to 2.2.0 allows any authenticated user to accept or reject friend

## Risk And Classification

**Primary CVSS:** v3.1 8.3 HIGH from nvd@nist.gov

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

**EPSS:** 0.000420000 probability, percentile 0.129700000 (date 2026-04-02)

**Problem Types:** CWE-863 | CWE-863 CWE-863 Incorrect Authorization

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L
3.0	security@huntr.dev	Secondary	8.3	HIGH	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L
3.0	CNA	DECLARED	8.3	HIGH	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

Low

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

### CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

Low

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lollms	Lollms	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Parisneo	Parisneo/lollms	affected unspecified 2.2.0 custom	Not specified

### References

Reference	Source	Link	Tags
huntr.com/bounties/6aab01ca-a138-4a1d-bef9-3bce145359bf	security@huntr.dev	huntr.com	Exploit, Issue Tra
github.com/parisneo/lollms/commit/c46297799f8e1e23305373f8350746b905e0e83c	security@huntr.dev	github.com	Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	vulnlist.com	canonical, analy

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](#).

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