Insecure Direct Object Reference (IDOR) in parisneo/lollms

MITRE | NVD | CVE.ORG | Print: PDF

Summary

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

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

ntegrity

High

vailability

Low

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

CVSS v3.0 Breakdown

ttack Vector

Network

ttack Complexity

Low

rivileges Required

Low

ser Interaction

None

cope

Unchanged

onfidentiality

High

ntegrity

High

vailability

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	nvd.nist.gov	canonical, analys

NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

No vendor comments have been submitted for this CVE.

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