Improper Access Control via Weak JWT Token in parisneo/lollms

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-1114
State	PUBLISHED
Assigner	@huntr_ai
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 07:16:23 UTC
Updated	2026-04-07 14:16:18 UTC
Description	In parisneo/lollms version 2.1.0, the application's session management is vulnerable to improper access control due to the u

Risk And Classification

Primary CVSS: v3.0 9.8 CRITICAL from security@huntr.dev

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

EPSS: 0.000450000 probability, percentile 0.137210000 (date 2026-04-07)

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

Version	Source	Type	Score	Severity	Vector
3.0	security@huntr.dev	Secondary	9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.0	CNA	DECLARED	9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

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
huntr.com/bounties/608b2a3b-2225-438e-9e61-ffbfdec2ed89	134c704f-9b21-4f2e-91b3-4a467353bcc0	huntr.com
github.com/parisneo/lollms/commit/a3b2b82b84d537a9da63e63a370a6a8ad55fed34	security@huntr.dev	github.cor
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

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