Arbitrary File Read via Prompt Tag Source Validation Bypass in mlflow/mlflow

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

Summary

CVE	CVE-2026-2614
State	PUBLISHED
Assigner	@huntr_ai
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-11 20:25:41 UTC
Updated	2026-05-13 15:53:49 UTC
Description	A vulnerability in the `_create_model_version()` handler of `mlflow/server/handlers.py` in mlflow/mlflow versions 3.9.0 and e

Risk And Classification

Primary CVSS: v3.0 7.5 HIGH from security@huntr.dev

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

EPSS: 0.000400000 probability, percentile 0.121970000 (date 2026-05-14)

Problem Types: CWE-22 | CWE-22 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
3.0	security@huntr.dev	Secondary	7.5	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.0	CNA	DECLARED	7.5	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mlflow	Mlflow/mlflow	affected unspecified 3.10.0 custom	Not specified

References

Reference	Source	Link
github.com/mlflow/mlflow/commit/6e801f4259d96804c73107315b24cef0f6aa115a	security@huntr.dev	github.com
huntr.com/bounties/19380271-3fbf-4beb-987e-6fd7069c55e6	134c704f-9b21-4f2e-91b3-4a467353bcc0	huntr.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.