Privilege Escalation in mlflow/mlflow

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

Summary

CVE	CVE-2025-10279
State	PUBLISHED
Assigner	@huntr_ai
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-02 11:16:16 UTC
Updated	2026-04-14 14:57:42 UTC
Description	In mlflow version 2.20.3, the temporary directory used for creating Python virtual environments is assigned insecure world-v

Risk And Classification

Primary CVSS: v3.0 7 HIGH from security@huntr.dev

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

Problem Types: CWE-379 | CWE-379 CWE-379 Creation of Temporary File in Directory with Insecure Permissions

Version	Source	Type	Score	Severity	Vector
3.0	security@huntr.dev	Secondary	7	HIGH	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
3.0	CNA	DECLARED	7	HIGH	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lfprojects	Mlflow	All	-	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mlflow	Mlflow/mlflow	affected unspecified 3.4.0 custom	Not specified

References

Reference	Source	Link	Tags
huntr.com/bounties/01d3b81e-13d1-43aa-b91a-443aec68bdc8	security@huntr.dev	huntr.com	Third Party Advisory
github.com/mlflow/mlflow/commit/1d7c8d4cf0a67d407499a8a4ffac387ea4f8194a	security@huntr.dev	github.com	Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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