Incomplete Fix for CVE-2025-10279: Insecure Temporary Directory Permissions in mlflow/mlflow

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

Summary

CVE	CVE-2026-4137
State	PUBLISHED
Assigner	@huntr_ai
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-18 21:16:40 UTC
Updated	2026-05-18 21:16:40 UTC
Description	In mlflow/mlflow versions prior to 3.11.0, the `get_or_create_nfs_tmp_dir()` function in `mlflow/utils/file_utils.py` creates tem

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-378 | CWE-378 CWE-378 Creation of Temporary File 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

Integrity
High
Availability
High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mlflow	Mlflow/mlflow	affected unspecified 3.11.0 custom	Not specified

References

Reference	Source	Link	Tags
github.com/mlflow/mlflow/commit/1dcbb0c2fbd1f446c328830e601ca13a28219b8a	security@huntr.dev	github.com	
huntr.com/bounties/648dc30b-76c7-4433-86b8-f43d926fd8d6	security@huntr.dev	huntr.com	
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.