Command Injection in mlflow/mlflow

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-0596
State	PUBLISHED
Assigner	@huntr_ai
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-31 15:16:10 UTC
Updated	2026-04-01 14:24:02 UTC
Description	A command injection vulnerability exists in mlflow/mlflow when serving a model with `enable_mlserver=True`. The `model_u

Risk And Classification

Primary CVSS: v3.0 9.6 CRITICAL from security@huntr.dev

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

EPSS: 0.002410000 probability, percentile 0.473390000 (date 2026-04-02)

Problem Types: CWE-78 | CWE-78 CWE-78 Improper Neutralization of Special Elements used in an OS Command

Version	Source	Type	Score	Severity	Vector
3.0	security@huntr.dev	Secondary	9.6	CRITICAL	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
3.0	CNA	DECLARED	9.6	CRITICAL	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v3.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

High

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

Vendor Declared Affected Products

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

References

Reference	Source	Link	Tags
huntr.com/bounties/2e905add-f9f5-4309-a3db-b17de5981285	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.