



Server-Side Request Forgery (SSRF) in mflow/mlflow

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-2393
State	PUBLISHED
Assigner	@huntr_ai
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-11 18:16:31 UTC
Updated	2026-05-13 15:53:49 UTC
Description	A Server-Side Request Forgery (SSRF) vulnerability exists in MLflow versions prior to 3.9.0. The `_create_webhook()` func

Risk And Classification

Primary CVSS: v3.0 7.1 HIGH from security@huntr.dev

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

EPSS: 0.000310000 probability, percentile 0.089300000 (date 2026-05-14)

Problem Types: CWE-918 | CWE-918 CWE-918 Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
3.0	security@huntr.dev	Secondary	7.1	HIGH	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N
3.0	CNA	DECLARED	7.1	HIGH	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

Low

Availability

None

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/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/64aa0ab7207f9c649b59ba1a5f40d82196817389	security@huntr.dev	github.com
huntr.com/bounties/04ef100d-06b5-4a70-95b1-b7be23aa8150	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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)