

CVE-2026-66384

JFrog Artifactory Improper Limitation of a Pathname to a Restricted Directory Vulnerability

CISA KEV since Aug 27, 2026

Actively exploited

An authenticated user may write data outside the intended Docker cache path under specific remote-repository conditions.

EVRS 75 /100 Urgent priority	CVSS V3.1 5.3 Medium · NVD	EPSS 0.007 51.1st percentile · FIRST	CISA DEADLINE Sep 10, 2026 CISA federal deadline · Overdue by 42 days
---	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☒ KEV recency	Added to CISA KEV within the last 90 days
☒ EPSS	0.007 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 5.3	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
artifactory	< 7.146.35 ≥ 7.161.0 < 7.161.16	7.146.35 · 7.161.16	NVD

Sources

Vendor guidance	docs.jfrog.com/releases/docs/jfrog-security-advisories	docs.jfrog.com	docs.jfrog.com/releases/docs/artifactory-self-managed-releases
BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk	Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk
NVD	nvd.nist.gov/vuln/detail/CVE-2026-66384	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-57256	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-66384

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.