

CVE-2026-6973

Ivanti Endpoint Manager Mobile (EPMM) Improper Input Validation Vulnerability

CISA KEV since May 7, 2026

Actively exploited

An Improper Input Validation in Ivanti EPMM before versions 12.6.1.1, 12.7.0.1, and 12.8.0.1 allows a remotely authenticated user with administrative access to achieve remote code execution.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 7.2 High · NVD	EPSS 0.025 84.8th percentile · FIRST	CISA DEADLINE May 10, 2026 CISA federal deadline · Overdue by 5 months
---	--	--	--

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 year
☒ EPSS	0.025 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.2	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
endpoint manager mobile	< 12.6.1.1 12.7.0.0 12.8.0.0	12.6.1.1	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-36fg-ffjj-h5p6	Additional guidance	hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-Multiple-CVEs
hub.ivanti.com	hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-Multiple-CVEs?language=en_US	NVD	nvd.nist.gov/vuln/detail/CVE-2026-6973
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-28396
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-6973		

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