

CVE-2025-4427

Ivanti Endpoint Manager Mobile (EPMM) Authentication Bypass Vulnerability

CISA KEV since May 19, 2025

Actively exploited

Public exploit module (Metasploit)

An authentication bypass in the API component of Ivanti Endpoint Manager Mobile 12.5.0.0 and prior allows attackers to access protected resources without proper credentials via the API.

EVRS 85 /100 Immediate priority	CVSS V3.1 7.5 High · NVD	EPSS 0.999 99.97th percentile · FIRST	CISA DEADLINE Jun 9, 2025 KEV since 2025 · listed over a year
--	--	---	---

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 two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately 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	< 11.12.0.5 ≥ 12.3.0.0 < 12.3.0.2 ≥ 12.4.0.0 < 12.4.0.2 12.5.0.0	11.12.0.5 · 12.3.0.2 · 12.4.0.2	NVD

Sources

Vendor guidance	forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM	NVD	nvd.nist.gov/vuln/detail/CVE-2025-4427
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-14388
Current data	evulnable.com/vulnerability-management/cve/CVE-2025-4427		

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