

CVE-2024-13161

Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability

CISA KEV since Mar 10, 2025

Actively exploited

Absolute path traversal in Ivanti EPM before the 2024 January-2025 Security Update and 2022 SU6 January-2025 Security Update allows a remote unauthenticated attacker to leak sensitive information.

EVRS 82 / ₁₀₀ Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.898 99.79th percentile · FIRST	CISA DEADLINE Mar 31, 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	0.898 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ 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	< 2022 2022 2024	2022	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-5fwx-95cc-hcxv	Additional guidance	forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6
forums.ivanti.com	forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6?language=en_US	NVD	nvd.nist.gov/vuln/detail/CVE-2024-13161
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-51387
Current data	evulnable.com/vulnerability-management/cve/CVE-2024-13161		

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