

CVE-2026-1603

Ivanti Endpoint Manager (EPM) Authentication Bypass Vulnerability

CISA KEV since Mar 9, 2026

Actively exploited

An authentication bypass in Ivanti Endpoint Manager before version 2024 SU5 allows a remote unauthenticated attacker to leak specific stored credential data.

EVRS 84 / ₁₀₀ Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.883 99.77th percentile · FIRST	CISA DEADLINE Mar 23, 2026 CISA federal deadline · Overdue by 7 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	0.883 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	< 2024 2024	2024	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-2j3g-j6qj-x9q2	Additional guidance	hub.ivanti.com/s/article/Security-Advisory-EPM-February-2026-for-EPM-2024?language=en_US
NVD	nvd.nist.gov/vuln/detail/CVE-2026-1603	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-6842	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-1603

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