

CVE-2024-29824

Ivanti Endpoint Manager (EPM) SQL Injection Vulnerability

CISA KEV since Oct 2, 2024

Actively exploited

Public exploit module (Metasploit)

An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.

EVRS 86 /100 Immediate priority	CVSS V3.1 8.8 High · NVD	EPSS 0.999 99.97th percentile · FIRST	CISA DEADLINE Oct 23, 2024 KEV since 2024 · 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	On the CISA KEV catalog for over two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions 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	2022	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-qz27-wgh8-6hcg	Additional guidance	forums.ivanti.com/s/article/Security-Advisory-May-2024
NVD	nvd.nist.gov/vuln/detail/CVE-2024-29824	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-26818	Current data	evulnable.com/vulnerability-management/cve/CVE-2024-29824

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