

CVE-2023-35078

Ivanti Endpoint Manager Mobile Authentication Bypass Vulnerability

Exigent

CISA KEV since Jul 25, 2023

Actively exploited

Ransomware use known

An authentication bypass vulnerability in Ivanti EPMM allows unauthorized users to access restricted functionality or resources of the application without proper authentication.

EVRS 94 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.99th percentile · FIRST	CISA DEADLINE Aug 15, 2023 KEV since 2023 · 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent 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 mobile	< 11.8.1.1 ≥ 11.9.0 < 11.9.1.1 ≥ 11.10 < 11.10.0.2	11.8.1.1 · 11.9.1.1 · 11.10.0.2	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-7r8j-4mv7-77vp	Additional guidance	forums.ivanti.com/s/article/CVE-2023-35078-Remote-unauthenticated-API-access-vulnerability
forums.ivanti.com	forums.ivanti.com/s/article/CVE-2023-35078-Remote-unauthenticated-API-access-vulnerability?language=en_US	NVD	nvd.nist.gov/vuln/detail/CVE-2023-35078
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-39113
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-35078		

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