CVE-2026-6973

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-6973
State	PUBLISHED
Assigner	ivanti
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-07 16:16:23 UTC
Updated	2026-05-07 19:18:39 UTC
Description	An Improper Input Validation in Ivanti EPMM before versions 12.6.1.1, 12.7.0.1, and 12.8.0.1 allows a remotely authenticate

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from 3c1d8aa1-5a33-4ea4-8992-aadd6440af75

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.050090000 probability, percentile 0.897880000 (date 2026-05-12)

CISA KEV: Listed on 2026-05-07; due 2026-05-10; ransomware use Unknown

Problem Types: CWE-20 | CWE-20 CWE-20 Improper input validation

Version	Source	Type	Score	Severity	Vector
3.1	3c1d8aa1-5a33-4ea4-8992-aadd6440af75	Secondary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CISA Known Exploited Vulnerability

Vendor	Ivanti
Product	Endpoint Manager Mobile (EPMM)
Name	Ivanti Endpoint Manager Mobile (EPMM) Improper Input Validation Vulnerability
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.
Notes	https://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-Multiple-CVEs?language=en_US ; https://nvd.nist.gov/vuln/detail/CVE-2026-6973

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ivanti	Endpoint Manager Mobile	All	All	All	All
Application	Ivanti	Endpoint Manager Mobile	12.7.0.0	All	All	All
Application	Ivanti	Endpoint Manager Mobile	12.8.0.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ivanti	Endpoint Manager Mobile	unaffected 12.6.1.1	Not specified
CNA	Ivanti	Endpoint Manager Mobile	unaffected 12.7.0.1	Not specified
CNA	Ivanti	Endpoint Manager Mobile	unaffected 12.8.0.1	Not specified

References

Reference	Source	Link
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.cisa.gov
hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-...	3c1d8aa1-5a33-4ea4-8992-aadd6440af75	hub.ivanti.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2026-05-07T00:00:00.000Z	CVE-2026-6973 added to CISA KEV

There are currently no legacy QID mappings associated with this CVE.