



# CVE-2026-6973

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-6973
<b>State</b>	PUBLISHED
<b>Assigner</b>	ivanti
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-07 16:16:23 UTC
<b>Updated</b>	2026-05-07 19:18:39 UTC
<b>Description</b>	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 authenticated user to execute arbitrary code on the affected system.

## 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

Integrity

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

<b>Vendor</b>	Ivanti
<b>Product</b>	Endpoint Manager Mobile (EPMM)
<b>Name</b>	Ivanti Endpoint Manager Mobile (EPMM) Improper Input Validation Vulnerability
<b>Required Action</b>	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
<b>Notes</b>	<a href="https://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-Multiple-CVEs?language=en_US">https://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-Multiple-CVEs?language=en_US</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2026-6973">https://nvd.nist.gov/vuln/detail/CVE-2026-6973</a>

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

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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)