Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Ivanti EPMM Flaws Threaten Enterprise Device Management Systems

Date of Publication	Admiralty Code	TA Number
May 08, 2026	A1	TA2026124

Summary

First Seen: May 2026
Affected Products: Ivanti Endpoint Manager Mobile (EPMM)
Impact: Ivanti has reported several high-severity vulnerabilities in Endpoint Manager Mobile (EPMM), including an actively exploited remote code execution flaw identified as CVE-2026-6973. These vulnerabilities could enable attackers to escalate privileges, bypass access controls, impersonate trusted components, and compromise device enrollment processes within enterprise environments. Security researchers believe that some of these flaws could be combined to achieve full server compromise, which raises significant concerns for organizations that rely on EPMM for mobile device management. In light of reports of limited exploitation in the wild, immediate patching and remediation are strongly urged.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-6973	Ivanti Endpoint Manager Mobile (EPMM) Improper Input Validation Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	✓	✓	✓
CVE-2026-5786	Ivanti Endpoint Manager Mobile (EPMM) Improper Access Control Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	✗	✗	✓
CVE-2026-5787	Ivanti Endpoint Manager Mobile (EPMM) Improper Certificate Validation Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	✗	✗	✓
CVE-2026-5788	Ivanti Endpoint Manager Mobile (EPMM) Improper Access Control Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	✗	✗	✓
CVE-2026-7821	Ivanti Endpoint Manager Mobile (EPMM) Improper Certificate Validation Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	✗	✗	✓

Vulnerability Details

#1

Ivanti is warning that a new security flaw impacting Endpoint Manager Mobile (EPMM) has been exploited in limited attacks in the wild. The most serious issue, tracked as CVE-2026-6973, is a high-severity remote code execution vulnerability caused by improper input validation in EPMM versions prior to 12.6.1.1, 12.7.0.1, and 12.8.0.1. The flaw allows a remote attacker with administrative privileges to execute arbitrary code on the vulnerable server without requiring user interaction. Although exploitation requires admin-level access, Ivanti confirmed that the vulnerability has already been abused against a small number of customers.

#2

Another high-severity vulnerability, CVE-2026-5786, stems from improper access control and enables a low-privileged authenticated user to escalate privileges to administrator level. Affecting the same EPMM versions, the flaw exists because the application does not properly verify user permissions before granting access to administrative functions. While Ivanti has not observed active exploitation of this issue, it could play a critical role in an attack chain by providing the elevated privileges needed to exploit CVE-2026-6973.

#3

Ivanti also disclosed CVE-2026-5787, a certificate validation flaw that could allow an unauthenticated attacker to impersonate trusted Sentry hosts and obtain valid CA-signed client certificates. This weakness impacts the certificate issuance and registration process in EPMM and could compromise the trust model used in Ivanti Sentry integrations. In addition, CVE-2026-5788 allows unauthenticated attackers to invoke arbitrary application methods due to insufficient access restrictions, potentially exposing vulnerable systems to unauthorized access or reconnaissance attempts.

#4

A fifth vulnerability, CVE-2026-7821, affects environments using Apple Device Enrollment. The flaw allows unauthenticated attackers to enroll restricted devices and gain access to sensitive information related to the EPMM appliance. The issue is caused by improper certificate validation during the enrollment process, potentially enabling attackers to bypass device enrollment restrictions and undermine the integrity of managed device identities. Organizations are strongly urged to apply the patched versions (12.6.1.1, 12.7.0.1, or 12.8.0.1) immediately, rotate all administrative credentials, and conduct forensic reviews to determine whether exploitation has already occurred.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-6973	Ivanti EPMM (Before 12.6.1.1, 12.7.0.1, 12.8.0.1)	cpe:2.3:a:ivanti:endpoint_manager_mobile:*:*:*:*:*:*:*:*	CWE-20
CVE-2026-5786			CWE-284
CVE-2026-5787			CWE-295
CVE-2026-5788			CWE-284
CVE-2026-7821			CWE-295, CWE-306

Recommendations

Apply Ivanti EPMM Security Updates Immediately: Upgrade all on-premises Ivanti EPMM instances to the patched versions 12.6.1.1, 12.7.0.1, or 12.8.0.1 without delay. CVE-2026-6973 is confirmed to be under active exploitation, and CISA has mandated federal agencies apply fixes by May 10, 2026. Prioritize this as a Priority 1 action item given the confirmed zero-day status and the potential for full system compromise through remote code execution.

Rotate Administrative Credentials and Audit Admin Accounts: Review all accounts with administrative privileges in the EPMM dashboard and remove any unfamiliar or unnecessary admin accounts. Rotate all administrative passwords and invalidate active sessions and tokens immediately. Ivanti has specifically stated that customers who rotated credentials following the January 2026 CVE-2026-1281 and CVE-2026-1340 exploitation face significantly reduced risk from CVE-2026-6973, underscoring the importance of credential hygiene.

Restrict Network Access to EPMM Admin Interfaces: Implement strict network segmentation and access controls to limit exposure of the EPMM administrative interface. Use VPN allowlists, firewall rules, and multi-factor authentication (MFA) to ensure that only authorized personnel from trusted networks can access administrative functions. This compensating control is essential if immediate patching is not feasible and significantly reduces the attack surface for all five disclosed vulnerabilities.

Vulnerability Management and Ongoing Posture Assessment: Establish a continuous vulnerability management process that includes regular scanning of Ivanti EPMM deployments, prompt application of security patches, and inventory tracking of deployed versions. Evaluate the security posture of the broader MDM infrastructure and consider migration to Ivanti Neurons for MDM (cloud-based solution), which is not affected by these vulnerabilities. Maintain awareness of the Ivanti security advisory ecosystem, as the vendor has experienced a recurring pattern of zero-day exploitation across its product portfolio.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Execution	T1059: Command and Scripting Interpreter	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

https://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-Multiple-CVEs?language=en_US

References

https://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-Multiple-CVEs?language=en_US

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

May 08, 2026 • 09:00 AM

More at www.hivepro.com