Active Exploitation of Ivanti Endpoint Manager Mobile

TL;DR

Ivanti confirmed active exploitation of two zero-day vulnerabilities in Endpoint Manager Mobile (EPMM) that allow unauthenticated remote code execution.

A temporary RPM mitigation is available now, but affected systems should be treated as potentially compromised until verified or rebuilt. A permanent fix is expected with EPMM 12.8.0.0 later this quarter.

Overview

There are two actively exploited code injection vulnerabilities affecting Ivanti Endpoint Manager Mobile (EPMM). Tracked as CVE-2026-1281 and CVE-2026-1340, both flaws were abused as zero-days prior to disclosure and allow unauthenticated remote code execution on vulnerable EPMM appliances. The Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2026-1281 to its Known Exploited Vulnerabilities catalog and gave federal agencies until February 1, 2026, to patch.

Affected Products

The vulnerabilities impact Ivanti Endpoint Manager Mobile (EPMM) only.

Not impacted:

- Ivanti Endpoint Manager (EPM)
- Ivanti Neurons for MDM
- Ivanti cloud products
- Sentry appliances themselves (though Sentry access paths should still be reviewed)

Affected versions include:

- EPMM 12.5.0.x, 12.6.0.x, 12.7.0.x
- EPMM 12.5.1.0, 12.6.1.0

CVE-2026-1281 – Unauthenticated Remote Code Execution (CVSS 9.8)

- CVE-2026-1281 is a code injection vulnerability in Ivanti Endpoint Manager Mobile that allows a remote attacker to execute arbitrary commands without authentication or user interaction. Successful exploitation gives attackers direct

access to the EPMM appliance, exposing sensitive information stored within the platform.
- This includes administrator and user account details, email addresses, mobile device identifiers, IP addresses, phone numbers, and installed application data. If device location tracking is enabled, attackers may also gain access to GPS coordinates and nearby cell tower information.
- Beyond data access, attackers can use the EPMM API or web console to change configuration and authentication settings, increasing the risk of follow-on access and control.

CVE-2026-1340 – Unauthenticated Remote Code Execution (CVSS 9.8)

- CVE-2026-1340 is a separate code injection vulnerability in Ivanti Endpoint Manager Mobile that results in the same outcome - unauthenticated remote code execution on the EPMM appliance.
- Like CVE-2026-1281, exploitation requires no privileges or user interaction and allows attackers to run commands directly on the system. A compromised appliance may expose the same categories of sensitive data, including user and admin accounts, device metadata, and managed mobile device information.
- Attackers may also modify EPMM configurations through administrative interfaces, expanding the impact beyond the initial system compromise and affecting managed devices and authentication workflows.

Ivanti appliances are attractive targets because they sit where identity and internal systems overlap. Even when EPMM is isolated in a DMZ, the data it holds still makes it valuable to attackers. If your EPMM environment is internet-facing, please patch immediately.

Aspire Protects

- Apply Ivanti's RPM mitigation immediately for your EPMM version to block active exploitation. See Ivanti's advisory for guidance.
- **Patch** - Upgrade to EPMM 12.8.0.0 when available, as the RPM is temporary and does not persist through version upgrades.
- Review EPMM access logs for suspicious activity tied to application distribution endpoints, paying close attention to repeated 404 responses from external sources.
- Rebuild or restore EPMM if compromise is suspected and reset all associated credentials and certificates.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] - The attacker may exploit exposed Ivanti EPMM application distribution and file transfer endpoints to gain unauthenticated access over the network.

Execution

- Command and Scripting Interpreter [T1059] - Successful exploitation may have allowed the attacker to execute arbitrary commands directly on the EPMM appliance.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

These Ivanti Endpoint Manager Mobile (EPMM) vulnerabilities impact organizations across the following industries that rely on EPMM to manage and secure mobile devices:

- Finance
- Government
- Education
- Energy
- Healthcare
- Retail
- Technology
- Manufacturing

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security

professionals to identify and respond to threats across a broader attack surface.

- Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.

- Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Security Advisory Ivanti Endpoint Manager Mobile (EPMM) (CVE-2026-1281 & CVE-2026-1340)