NCA-05.030226 – National CERT Advisory – Active Exploitation of Critical Zero-Day Vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM)

INTRODUCTION

The National CERT has identified a **critical and actively exploited cybersecurity threat** affecting **Ivanti Endpoint Manager Mobile (EPMM)** on-premises appliances. Ivanti has confirmed the existence of **two zero-day remote code execution (RCE) vulnerabilities** that allow **unauthenticated attackers** to fully compromise vulnerable EPMM instances.

These flaws enable remote adversaries to execute arbitrary code without valid credentials or user interaction, resulting in **complete appliance takeover**, potential exposure of sensitive mobile device data, and compromise of enterprise or government mobile device management environments. Given confirmed exploitation in the wild and inclusion of one vulnerability in the **CISA Known Exploited Vulnerabilities (KEV) catalog**, **immediate action is mandatory**.

Threat Type: Remote Code Execution / Appliance Compromise
Severity: Critical
Attack Vector: Network-based, unauthenticated
Authentication Required: No
User Interaction: None
CVSS (Base): 9.8 (Critical – Confidentiality, Integrity, Availability Impact)

IMPACT

Successful exploitation of these vulnerabilities may result in:

1. **Complete System Compromise** – Full administrative control of EPMM appliances
2. **Sensitive Data Exposure** – Access to managed mobile device data and credentials
3. **Policy Manipulation** – Unauthorized modification of device configurations and security policies
4. **Persistent Backdoor Deployment** – Long-term unauthorized access
5. **Lateral Movement** – Pivoting into internal enterprise or government networks
6. **Operational Disruption** – Loss of mobile device management capabilities
7. **Compliance Violations** – Breach of regulatory and data protection obligations
8. **Supply Chain Risk** – Abuse of trusted management infrastructure
9. **Espionage Enablement** – Targeting of government or critical sector mobile assets
10. **Reputational Damage** – Loss of trust due to infrastructure compromise

THREAT DETAILS

Threat Overview

- **Threat Category:** Zero-day Remote Code Execution
- **Threat Status:** Actively exploited in the wild
- **Root Cause:** Improper input handling leading to code injection
- **Exploit Maturity:** Weaponized
- **Persistence Risk:** High (attackers may implant backdoors)

Vulnerability Information

- **CVE-2026-1281** – Critical unauthenticated code injection (CISA KEV-listed)
- **CVE-2026-1340** – Critical unauthenticated code injection
- **Affected Functionality:**
    - In-House Application Distribution
    - Android File Transfer Configuration

Likely CWE

- CWE-94 – Improper Control of Code Generation
- CWE-77 – Command Injection
- CWE-284 – Improper Access Control

AFFECTED SYSTEMS / PLATFORMS

Impacted Products

- Ivanti Endpoint Manager Mobile (EPMM) **on-premises appliances**

Affected Versions

- EPMM 12.5.0.0 and earlier
- EPMM 12.5.1.0 and earlier
- EPMM 12.6.0.0 and earlier
- EPMM 12.6.1.0 and earlier
- EPMM 12.7.0.0 and earlier

Not Affected

- Ivanti Neurons for MDM
- Ivanti Endpoint Manager (EPM)
- Ivanti Sentry

THREAT CHARACTERISTICS

- **Attack Vector:** Remote network access
- **Attack Complexity:** Low

- **Privileges Required:** None
- **User Interaction:** None
- **Exploit Scope:** Complete appliance compromise
- **Exposure Surface:** Internet-facing or externally reachable EPMM instances

INDICATORS OF EXPLOITATION (IoEs)

Category	Indicator	Description	Action Required
Network	Suspicious HTTP/S requests to EPMM endpoints	Possible exploit attempts	Investigate
Logs	Unexpected command execution events	Active compromise	Incident response
System	New or modified admin accounts	Unauthorized access	Contain
Config	Altered policies or settings	Integrity violation	Audit
Filesystem	Unknown scripts or binaries	Backdoor presence	Forensic review
HA Nodes	Inconsistent patch levels	Exposure risk	Patch immediately
Firewall	Traffic from unknown IPs	External exploitation	Block
IDS/IPS	Exploit signatures triggered	Active attack	Escalate
Monitoring	Sudden configuration changes	Malicious activity	Investigate
Security	CISA KEV correlation	Known exploited vulnerability	Immediate action

AFFECTED USERS / ENVIRONMENTS

- Government and critical infrastructure organizations
- Enterprises using Ivanti EPMM on-premises
- Mobile device administrators and MDM teams
- Environments managing sensitive or regulated mobile data
- Internet-exposed or DMZ-deployed EPMM appliances

REMEDIATION ACTIONS

1. Immediate Patching (MANDATORY)

- Apply Ivanti's **emergency RPM patches immediately**
- Patch **all nodes**, including High Availability (HA) members
- Prioritize **internet-facing appliances**
- Verify patch application and system integrity

Note: Patching does not require downtime.

2. Permanent Remediation

- Plan upgrade to **EPMM version 12.8.0.0** upon release
- Reapply RPM patches after upgrades if required

3. Interim Mitigations (If Patching Is Delayed)

- Isolate EPMM appliances from untrusted networks
- Restrict access via firewall rules and segmentation
- Monitor logs for anomalous behavior
- Review administrator accounts and authentication settings

Mitigations do not eliminate risk. Patching is the only complete remediation.

ACTION SUMMARY & RESPONSE PRIORITIES

Action Type	Specific Steps	Priority	Timeframe
Patching	Apply emergency RPM fixes	**MANDATORY**	Immediate
Exposure Reduction	Restrict external access	HIGH	Immediate
Monitoring	Enable enhanced logging	HIGH	Immediate
Upgrade	Move to EPMM 12.8.0.0	REQUIRED	Q1 2026
Validation	Audit HA environments	REQUIRED	Immediate
Incident Response	Investigate compromise indicators	CRITICAL	Ongoing

MONITORING & DETECTION

Organizations should:

- Continuously monitor EPMM access logs
- Alert on unauthenticated or anomalous requests
- Review configuration and policy changes
- Correlate activity with known exploitation patterns
- Conduct compromise assessments if exposure is confirmed

REFERENCES

1. https://nvd.nist.gov/vuln/detail/CVE-2026-1281
2. https://nvd.nist.gov/vuln/detail/CVE-2026-1340
3. https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US

CALL TO ACTION

The National CERT **strongly urges** all organizations operating Ivanti EPMM to:

1. **Patch immediately** without exception

2. **Assume compromise** if systems were exposed and unpatched
3. **Audit for indicators of exploitation**
4. **Restrict unnecessary external access**
5. **Prepare incident response actions** if malicious activity is detected

Failure to act may result in **complete infrastructure compromise, sensitive data exposure, regulatory violations, and long-term operational risk**.