INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-07 19:05 UTC

Ivanti EPMM Patch Bundle: Active RCE Exploitation (CVE-2026-6973) Plus Three Unauthenticated Attack Vectors

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0141
Type	CVE Vulnerability
CVE ID	CVE-2026-6973, CVE-2026-5786, CVE-2026-5787, CVE-2026-5788, CVE-2026-7821, CVE-2026-1281, CVE-2026-1340
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Ivanti Endpoint Manager Mobile (EPMM) on-premises versions prior to 12.6.1.1, 12.7.0.1, and 12.8.0.1
Published	2026-05-07T13:55:00
Discovery Source	Rss

Executive Summary

Ivanti has confirmed active exploitation of a remote code execution vulnerability (CVE-2026-6973) in Endpoint Manager Mobile, the platform organizations use to manage and secure corporate mobile devices. CISA added this flaw to its Known Exploited Vulnerabilities catalog with a federal remediation deadline of May 10, 2026, and the broader patch bundle covers six additional CVEs, at least two of which require no authentication to exploit. Because EPMM stores privileged credentials, device certificates, and enterprise network access configurations, a successful attack can give adversaries a direct path into the broader corporate environment.

Technical Analysis

Ivanti Endpoint Manager Mobile (EPMM) on-premises is affected by a seven-CVE patch bundle. CVE-2026-6973 is an authenticated RCE flaw; vendor advisory cites CVSS 7.2, but aggregated scoring across the full patch bundle reaches 9.5 due to unauthenticated attack vectors in the bundle. Individual per-CVE CVSS scores and vectors are pending NVD publication. For operational triage, treat the bundle as critical due to confirmed active exploitation and CISA KEV listing with a May 10, 2026 remediation deadline; do not wait for final CVSS confirmation before patching. EPSS scores are not yet available and will be populated once NVD entries are finalized. Two or more additional CVEs in the bundle (CVE-2026-5786, CVE-2026-5787,

CVE-2026-5788, CVE-2026-7821, CVE-2026-1281, CVE-2026-1340) are unauthenticated attack vectors, materially expanding exploitable surface. Underlying weakness classes: CWE-20 (improper input validation), CWE-284 (improper access control), CWE-295 (improper certificate validation). Relevant MITRE ATT&CK techniques include T1190 (Exploit Public-Facing Application), T1078 (Valid Accounts), T1552 (Unsecured Credentials), T1550 (Use Alternate Authentication Material), T1133 (External Remote Services), T1210 (Exploitation of Remote Services), T1609 (Container Administration Command), T1556 (Modify Authentication Process), and T1068 (Exploitation for Privilege Escalation). Affected versions: all EPMM on-premises releases prior to 12.6.1.1, 12.7.0.1, and 12.8.0.1. Ivanti cloud-hosted instances are not affected. Additional CVE IDs in the patch bundle have individual NVD entries; primary reference is CVE-2026-6973. Source: Ivanti May 2026 Security Advisory (vendor); CISA Known Exploited Vulnerabilities (federal authority); BleepingComputer and The Hacker News (technology news tier).

Action Checklist

1. Step 1: Containment, Immediately identify all on-premises EPMM instances running versions prior to 12.6.1.1, 12.7.0.1, or 12.8.0.1. If patching cannot begin within 24 hours, restrict inbound access to the EPMM management interface to known administrative IP ranges; block external access at the perimeter for any internet-exposed EPMM portals. Ivanti advisory reference: May 2026 Security Advisory for EPMM.
2. Step 2: Detection, Review EPMM application and web server logs for anomalous POST requests to administrative API endpoints, unexpected process spawning from the EPMM service account, and certificate validation errors (CWE-295 indicator). Query your SIEM for authentication events against EPMM from unfamiliar source IPs, especially successful logins followed immediately by configuration changes. Check EDR telemetry on the EPMM host for child process creation from the Java runtime or application server process. No public IOCs are confirmed at this time; treat any unrecognized authenticated session on EPMM as suspicious until patched.
3. Step 3: Eradication, Apply Ivanti's patched releases: 12.6.1.1, 12.7.0.1, or 12.8.0.1, corresponding to your current version branch. Follow Ivanti's upgrade path documented in the May 2026 Security Advisory. Do not skip intermediate versions if your upgrade path requires staged updates. After patching, rotate all service account credentials, API keys, and certificates stored within or managed by EPMM. Consult Ivanti's patch notes for automated credential rotation tooling; if unavailable, manually rotate service account passwords, API keys, and device certificates through the EPMM admin console. These are primary post-exploitation targets.
4. Step 4: Recovery, After patching, validate the EPMM version string in the admin console confirms the target release. Run Ivanti's integrity verification tooling if available. Monitor EPMM authentication logs and managed device enrollment activity for 72 hours post-patch for signs of persistence (unexpected device re-enrollments, credential reuse from unfamiliar hosts). Confirm managed endpoint certificates have not been tampered with by auditing certificate issuance logs.
5. Step 5: Post-Incident, This incident exposes two recurring control gaps: internet-exposed mobile device management (MDM) interfaces without network-layer access restrictions, and delayed patch cycles for internet-facing management platforms. Implement a network policy requiring MDM admin interfaces to be accessible only from management VLANs or VPN. Establish an SLA for CISA KEV-listed vulnerabilities on internet-facing systems of 48-72 hours. Review your asset inventory process to ensure all EPMM on-premises instances are discovered and tracked; shadow deployments are a common gap in MDM environments.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, legal, and breach notification counsel immediately if EPMM audit logs show any successful unauthenticated API access, unauthorized certificate issuance, unauthorized admin account creation, or if managed device count under EPMM includes devices enrolled with access to regulated data (PII, PHI, PCI-DSS cardholder data), as EPMM's role as the trust anchor for managed device certificates and credentials means a confirmed compromise constitutes a privileged credential breach with potential regulatory notification obligations.
Recovery Notes	Post-patch recovery must treat all credentials, API keys, and MDM certificates that existed in EPMM prior to patching as fully compromised and rotate them unconditionally — do not attempt to assess whether individual credentials were accessed, as the unauthenticated attack vectors (CVE-2026-5786, CVE-2026-5787, CVE-2026-5788) may have enabled silent exfiltration without leaving attributable authentication events. Monitor EPMM enrollment activity and certificate issuance for a minimum of 72 hours post-patch, extending to 7 days if any confirmed exploitation indicators were found during detection, given the risk of attacker-enrolled rogue devices persisting in the MDM environment. Validate the integrity of all managed endpoint MDM profiles by forcing a device check-in cycle and auditing the resulting enrollment log for any device IDs not present in the pre-incident asset inventory.
Forensic Artifacts	EPMM Tomcat access logs (localhost_access_log.*.txt at C:\Program Files\MobileIron\Core\tomcat\logs\ or /opt/mobileiron/core/tomcat/logs/) — unauthenticated exploitation of CVE-2026-5786/5787/5788 produces HTTP 200 responses to administrative API endpoints (/mifs/, /api/v2/) with no preceding session authentication event in the same source IP session stream | EPMM application log (mi.log at /opt/mobileiron/core/logs/ or Windows equivalent) — CVE-2026-6973 RCE via improper certificate validation (CWE-295) produces SSLHandshakeException, CertPathValidatorException, or PKIX path building errors immediately preceding unexpected process spawn events from the Java runtime | Sysmon Event ID 1 (Process Creation) on the EPMM host — RCE exploitation of CVE-2026-6973 manifests as cmd.exe, powershell.exe, or sh spawned with parent process matching the EPMM Java runtime (java.exe or wrapper.exe under the MobileIron/Core installation path), which is not a legitimate operational behavior for the EPMM service | EPMM database (PostgreSQL) audit and transaction logs — post-exploitation privilege abuse targeting EPMM's credential store would appear as unauthorized SELECT or COPY operations against tables storing device certificates, API keys, or service account credentials, and as INSERT events creating new admin accounts or API keys outside normal provisioning windows | EPMM Admin Console certificate issuance log (Admin > Certificate Management > Issued Certificates) and device enrollment records — a confirmed compromise of EPMM's MDM CA trust chain (the primary post-exploitation target given EPMM's role) leaves forensic evidence as certificate issuance events for unrecognized device IDs or user accounts, and rogue device enrollment records that persist even after the EPMM vulnerability is patched

Per-Action IR Details

Step 1: Containment — Immediately identify all on-premises EPMM instances running versions prior to 12.6.1.1, 12.7.0.1, or 12.8.0.1. If patching cannot begin within 24 hours, restrict inbound access to the EPMM management interface to known administrative IP ranges; block external access at the perimeter for any internet-exposed EPMM portals. Ivanti advisory reference: May 2026 Security Advisory for EPMM.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment, Eradication, and Recovery: Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Use netstat -ano on the EPMM Windows host to enumerate all listening ports associated with the Ivanti EPMM service (default: TCP 443, 8443, 9090). On the perimeter firewall or host-based Windows Firewall, add explicit DENY rules for all source IPs not in the admin IP allowlist: netsh advfirewall firewall add rule name='EPMM-BLOCK-EXTERNAL' dir=in action=block protocol=tcp localport=443,8443,9090. For Linux-hosted EPMM, use iptables -I INPUT -p tcp --dport 443 -j DROP followed by explicit ACCEPT rules per admin IP. Validate with a port scan from an external IP using nmap -p 443,8443,9090 [EPMM-IP] to confirm block is effective before proceeding.

Evidence: Before applying network blocks, capture the current EPMM connection state: run ss -tnp or netstat -anp on the EPMM host and save output to a timestamped file to document any active sessions at time of containment. Export perimeter firewall connection logs for the 30 days prior covering inbound traffic to the EPMM management interface ports (443, 8443, 9090) — these establish the pre-containment attacker access window. Capture the running EPMM process list (tasklist /v on Windows or ps aux on Linux) and save to preserve baseline process state before any changes are made. Document the EPMM version string from the admin console (Admin > System Info) as a timestamped screenshot to confirm scope.

Step 2: Detection — Review EPMM application and web server logs for anomalous POST requests to administrative API endpoints, unexpected process spawning from the EPMM service account, and certificate validation errors (CWE-295 indicator). Query your SIEM for authentication events against EPMM from unfamiliar source IPs, especially successful logins followed immediately by configuration changes. Check EDR telemetry on the EPMM host for child process creation from the Java runtime or application server process. No public IOCs are confirmed at this time; treat any unrecognized authenticated session on EPMM as suspicious until patched.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Signs of an Incident and Incident Analysis

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM or EDR, deploy Sysmon on the EPMM Windows host using a community config (SwiftOnSecurity template) with ProcessCreate (Event ID 1) and NetworkConnect (Event ID 3) logging enabled — focus on the EPMM service account (typically 'SYSTEM' or a dedicated service account) spawning cmd.exe, powershell.exe, or wscript.exe. Parse EPMM's Tomcat-based access log (default path: C:\Program Files\MobileIron\Core\tomcat\logs\localhost_access_log.*.txt or /opt/mobileiron/core/tomcat/logs/ on Linux) using PowerShell: Select-String -Path 'localhost_access_log.*.txt' -Pattern 'POST.*/mifs/|POST.*/api/v[0-9]' | Where-Object { $_ -match '(20[2-9]|[3-5][0-9][0-9]) ' } to extract POST requests returning success codes. For certificate anomalies (CWE-295), grep EPMM application logs for 'SSLHandshakeException' or 'CertPathValidatorException': grep -E 'SSLHandshakeException|CertPathValidatorException|PKIX path' /opt/mobileiron/core/logs/mi.log. Map findings against MITRE ATT&CK T1190 (Exploit Public-Facing Application) and T1078 (Valid Accounts) for session hijack follow-on.

Evidence: Collect EPMM Tomcat access logs (localhost_access_log.*.txt) and application logs (mi.log, server.log) covering the 30-day window prior to detection — unauthenticated CVE-2026-5786, CVE-2026-5787, and CVE-2026-5788 exploitation would appear as successful HTTP 200 responses to API endpoints with no prior authentication event in the same session. From Sysmon Event ID 1 (Process Creation), filter for parent process matching the Ivanti EPMM Java executable (wrapper.exe or java.exe under the MobileIron/Core path) spawning unexpected children — RCE via CVE-2026-6973 would manifest here. Capture Windows Security Event Log Event ID 4624 (Successful Logon) and 4648 (Explicit Credential Use) for the EPMM service account to identify lateral movement post-exploitation. Export EPMM audit logs from the admin console (Logs > Audit Logs) for admin API actions, configuration changes, and device enrollment events in the exploitation window. Collect Sysmon Event ID 3 (Network Connection) for outbound connections from the EPMM Java process to unexpected external IPs, which would indicate post-exploitation C2 staging.

Step 3: Eradication — Apply Ivanti's patched releases: 12.6.1.1, 12.7.0.1, or 12.8.0.1, corresponding to your current version branch. Follow Ivanti's upgrade path documented in the May 2026 Security Advisory. Do not skip intermediate versions if your upgrade path requires staged updates. After patching, rotate all service account credentials, API keys, and certificates stored within or managed by EPMM, as these are primary post-exploitation targets.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Containment, Eradication, and Recovery: Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST IR-4 (Incident Handling), NIST IA-5 (Authenticator Management), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 5.2 (Use Unique Passwords)

Compensating: Before applying the patch, take a full snapshot or offline backup of the EPMM VM to preserve forensic state — do not patch over potential evidence without this step. Verify the Ivanti patch installer SHA-256 hash against the value published in the May 2026 Security Advisory before execution: Get-FileHash -Algorithm SHA256 -Path .\EPMM_upgrade_12.x.x.x.zip. Post-patch, use the EPMM admin console's built-in certificate management section to identify all MDM push certificates, APNs certificates, and SCEP profiles — export a list before and after rotation to confirm full coverage. For API key rotation where no automated tooling exists, query the EPMM database directly (with vendor documentation guidance) or use the REST API: GET /api/v2/tenant/apikey to enumerate issued keys, then revoke and reissue. For service account password rotation, use the EPMM Local User Management console and enforce a minimum 20-character random password via PowerShell: -join ((65..90)+(97..122)+(48..57) | Get-Random -Count 20 | % {[char]$_}).

Evidence: Before applying the patch, preserve a memory dump of the EPMM server process using ProcDump (Sysinternals): procdump -ma [EPMM-PID] epmm_predpatch.dmp — this captures any in-memory webshells or injected code that would be lost after service restart during patching. Collect the full contents of the EPMM web application directory (C:\Program Files\MobileIron\Core\tomcat\webapps\ or Linux equivalent) and hash every file with Get-FileHash -Recurse or sha256sum -r to detect any webshell implants dropped via CVE-2026-6973 RCE. Check EPMM's database (typically PostgreSQL) transaction logs for unauthorized schema changes, new admin account creation, or API key issuance events that occurred during the suspected exploitation window — query: SELECT * FROM audit_log WHERE event_time > '[exploitation_start]' ORDER BY event_time ASC. Export the full list of currently enrolled MDM certificates and device enrollment records as a baseline before rotation to enable post-eradication comparison.

Step 4: Recovery — After patching, validate the EPMM version string in the admin console confirms the target release. Run Ivanti's integrity verification tooling if available. Monitor EPMM authentication logs and managed device enrollment activity for 72 hours post-patch for signs of persistence (unexpected device re-enrollments, credential reuse from unfamiliar hosts). Confirm managed endpoint certificates have not been tampered with by auditing certificate issuance logs.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Containment, Eradication, and Recovery: Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-11 (Audit Record Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Verify the patched EPMM version via the REST API without relying solely on the admin console UI (which could be spoofed by a persistent implant): curl -sk https://[EPMM-IP]/mifs/j_spring_security_check and inspect the Server response header, or query GET /api/v2/system/license for version metadata. For integrity verification without Ivanti's proprietary tooling, use a YARA rule targeting known JSP webshell signatures scanned against the EPMM webapps directory: yara -r webshell_rules.yar /opt/mobileiron/core/tomcat/webapps/ (community rules available from Neo23x0/signature-base on GitHub — note: verify rule source independently). Monitor EPMM enrollment logs for 72 hours using a scheduled task: every 4 hours, run Get-Content EPMM_enrollment.log | Select-String 'NEW_ENROLLMENT|DEVICE_REGISTERED' and diff against the pre-patch baseline enrollment list. Alert on any delta.

Evidence: During recovery monitoring, collect EPMM certificate issuance logs (Admin > Certificate Management > Issued Certificates) and diff against the pre-eradication baseline export — unauthorized certificate issuance by an attacker using stolen EPMM CA credentials (a direct consequence of EPMM's privileged credential storage) would appear as new entries for unrecognized devices or users. Capture Sysmon Event ID 11 (File Create) on the EPMM host for 72 hours post-patch to detect webshell re-deployment attempts via any persistence mechanism that survived eradication. Monitor EPMM's outbound network connections (Sysmon Event ID 3) for the Java process contacting external IPs not in the Ivanti cloud services allowlist — post-exploitation persistence via scheduled tasks or implants would generate beaconing behavior here. Preserve all EPMM authentication logs (successful and failed) for the 72-hour monitoring window under NIST AU-11 (Audit Record Retention) retention requirements for potential legal or regulatory review.

Step 5: Post-Incident — This incident exposes two recurring control gaps: internet-exposed mobile device management (MDM) interfaces without network-layer access restrictions, and delayed patch cycles for internet-facing management platforms. Implement a network policy requiring MDM admin interfaces to be accessible only from management VLANs or VPN. Establish an SLA for CISA KEV-listed vulnerabilities on internet-facing systems of 48-72 hours. Review your asset inventory process to ensure all EPMM on-premises instances are discovered and tracked — shadow deployments are a common gap in MDM environments.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons Learned and Evidence Retention

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-3 (Risk Assessment), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access)

Compensating: For shadow EPMM instance discovery without an enterprise asset management platform, run an internal network scan using nmap -p 443,8443,9090 --open -sV 10.0.0.0/8 | grep -i 'mobileiron\|ivanti\|mifs' to fingerprint EPMM service banners across all RFC-1918 space. For CISA KEV SLA enforcement without a vulnerability management platform, create a weekly cron job or scheduled task that pulls the CISA KEV JSON feed (https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json — validate this URL independently before use) and diffs it against your EPMM asset list, alerting when a KEV match is found. Document the lessons-learned output from this incident in a structured format per NIST 800-61r3 §4.1 and distribute to IT asset owners, network, and IAM teams — specifically the finding that EPMM's privileged credential store makes it a Tier-1 target requiring the same patch SLA as domain controllers.

Evidence: For the post-incident lessons-learned record, preserve: the timeline of EPMM version discovery across all instances (proving asset inventory gaps), the firewall rule change timestamps showing when external access was blocked (proving delayed network segmentation), and the delta between CISA KEV listing date and your organization's patch application date (quantifying SLA gap). Retain all collected forensic artifacts (Tomcat access logs, Sysmon logs, memory dumps, certificate issuance records) for a minimum of 12 months per NIST AU-11 (Audit Record Retention) or applicable regulatory retention requirements, as EPMM's management of mobile device credentials and certificates may implicate breach notification obligations for managed endpoint data. Document whether any managed device MDM certificates were issued or revoked during the exploitation window, as compromised MDM certificates could enable persistent access to managed endpoints even after EPMM is patched — this is the long-tail risk specific to MDM platform compromises.

Detection Guidance

No confirmed public IOCs (IPs, domains, hashes) are available at this time. Detection should focus on behavioral indicators. On the EPMM host: monitor for unexpected child processes spawned by the application server or Java runtime (T1190, T1609). In authentication logs: flag successful logins to the EPMM admin interface from IPs outside your known administrative ranges, particularly when followed by configuration changes or certificate operations (T1078, T1550, T1556). In network logs: look for unauthenticated requests to

EPMM API endpoints that return 200 responses, which may indicate exploitation of the unauthenticated CVEs in the bundle (T1133, T1210). In credential stores: alert on any access to credentials or certificates managed by EPMM outside normal MDM workflows (T1552). MITRE ATT&CK techniques T1190 and T1068 are primary indicators for initial access and privilege escalation. Cross-reference EPMM logs with your EDR for process injection or lateral movement originating from the EPMM server. Until NVD entries publish full technical details, treat all anomalous EPMM activity as high-priority pending investigation.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed public IOCs available at time of publication`	No specific IPs, domains, hashes, or URLs linked to active exploitation have been publicly disclosed. Monitor threat intelligence feeds for updates as NVD entries and incident reports publish.	LOW

Framework Mappings

MITRE-ATTACK

- **T1552** — Unsecured Credentials
- **T1609** — Container Administration Command
- **T1550** — Use Alternate Authentication Material
- **T1078** — Valid Accounts
- **T1133** — External Remote Services
- **T1210** — Exploitation of Remote Services
- **T1556** — Modify Authentication Process
- **T1190** — Exploit Public-Facing Application
- **T1068** — Exploitation for Privilege Escalation

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing

- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-10** — Information Input Validation
- **AC-3** — Access Enforcement
- **SC-8** — Transmission Confidentiality and Integrity
- **SC-17** — Public Key Infrastructure Certificates
- **SC-13** — Cryptographic Protection
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A01:2021** — Broken Access Control
- **A02:2021** — Cryptographic Failures
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **3.10** — Encrypt Sensitive Data in Transit
- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.26** — Application security requirements
- **A.8.8** — Management of technical vulnerabilities

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.312(d)** — Person or Entity Authentication

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1552	Unsecured Credentials	Credential-Access

Technique ID	Technique Name	Tactic
T1609	Container Administration Command	Execution
T1550	Use Alternate Authentication Material	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1133	External Remote Services	Persistence
T1210	Exploitation of Remote Services	Lateral-Movement
T1556	Modify Authentication Process	Credential-Access
T1190	Exploit Public-Facing Application	Initial-Access
T1068	Exploitation for Privilege Escalation	Privilege-Escalation

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/05/ivanti-epmm-cve-2026-6973-rce-und...	T3
Ivanti warns of new EPMM flaw exploited in zero-day attacks	https://www.bleepingcomputer.com/news/security/ivanti-warns-of-new-...	T3
May 2026 Security Advisory Ivanti Endpoint Manager Mobile (EPMM ...	https://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-...	T3
Ivanti Warns of Actively Exploited Zero-Day Flaw in Endpoint ...	https://www.techechelon.com/post/ivanti-warns-of-actively-exploited...	T3
Ivanti EPMM Zero■Day CVE■2026■6973: Admin■Authenticated RCE ...	https://threataft.com/articles/ivanti-epmm-zero-day-cve-2026-6973-a...	T2
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-6973, CVE-2026-5786, CVE-...	T1

Generated 2026-05-07 19:05 UTC by TJS Security Command Center