Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Ivanti Patches Actively Exploited EPMM Flaws

Date of Publication	Admiralty Code	TA Number
January 30, 2026	A1	TA2026030

Summary

First Seen: January 29, 2026
Affected Products: Ivanti Endpoint Manager Mobile (EPMM)
Impact: Ivanti has issued emergency security updates to fix two critical code injection flaws in Ivanti Endpoint Manager Mobile (EPMM), a widely used enterprise mobile device management platform, after confirming they were actively exploited. Tracked as CVE-2026-1281 and CVE-2026-1340, the vulnerabilities affect the In-House Application Distribution and Android File Transfer Configuration features, allowing unauthenticated remote attackers to execute arbitrary code on vulnerable on-premises EPMM appliances. While Ivanti reports that only a limited number of customers were impacted, the risk is significant. Successful exploitation could give attackers unauthenticated remote code execution and potentially use the compromised EPMM server as a foothold for lateral movement, especially in environments integrated with Ivanti Sentry. Ivanti clarified that cloud-hosted Ivanti Neurons for MDM and other Ivanti products are not affected and have released temporary RPM patches, with a permanent fix planned in EPMM version 12.8.0.0 later in Q1 2026.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-1281	Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	✓	✓	✓
CVE-2026-1340	Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	✓	✗	✓

Vulnerability Details

#1

CVE-2026-1281 and CVE-2026-1340 are both classified as code injection vulnerabilities under CWE-94 (Improper Control of Generation of Code). These critical security flaws reside within the In-House Application Distribution and Android File Transfer Configuration components of Ivanti Endpoint Manager Mobile. The root cause of these vulnerabilities stems from insufficient input validation and improper handling of user-supplied data within these specific features, allowing malicious input to be interpreted and executed as code on the underlying system.

#2

The exploitation mechanism enables unauthenticated remote attackers to inject and execute arbitrary code on vulnerable EPMM appliances without requiring any prior authentication or user interaction. The scope of impact extends to EPMM installations running versions 12.5.0.0 and prior, 12.5.1.0 and prior, 12.6.0.0 and prior, 12.6.1.0 and prior, and 12.7.0.0 and prior.

#3

Ivanti has confirmed active exploitation of these vulnerabilities, with evidence of attacks occurring before public disclosure. Successful exploitation attempts can be identified through the Apache HTTPD access log located at /var/log/httpd/https-access_log, where legitimate use produces 200 HTTP response codes while exploitation attempts result in 404 HTTP response codes. Organizations are advised to monitor for long-running connections initiated by the EPMM appliance in firewall logs as potential indicators of reverse shell activity.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-1281	Ivanti EPMM Versions 12.5.0.0 and prior, 12.6.0.0 and prior, 12.7.0.0 and prior, 12.5.1.0 and prior, 12.6.1.0 and prior	cpe:2.3:a:ivanti:endpoint_manager_mobile:12.5.0.0:*:*:*:*:*:*:* cpe:2.3:a:ivanti:endpoint_manager_mobile:12.6.0.0:*:*:*:*:*:*:* cpe:2.3:a:ivanti:endpoint_manager_mobile:12.7.0.0:*:*:*:*:*:*:* cpe:2.3:a:ivanti:endpoint_manager_mobile:12.5.1.0:*:*:*:*:*:*:* cpe:2.3:a:ivanti:endpoint_manager_mobile:12.6.1.0:*:*:*:*:*:*:*	CWE-94
CVE-2026-1340			CWE-94

Recommendations

Apply RPM Patch Immediately: All organizations with on-premises Ivanti EPMM installations must apply the provided RPM patch without delay. The patch does not require downtime and does not negatively affect any EPMM features. This is a provisional fix that addresses the immediate exploitation risk while a permanent solution is prepared.

Plan for Version 12.8.0.0 Upgrade: Ivanti has announced that the permanent fix for these vulnerabilities will be included in EPMM version 12.8.0.0, scheduled for release later. Organizations should begin planning for this upgrade immediately and adopt the new version once available to ensure comprehensive protection.

Reapply Patches After Version Upgrades: The RPM patch does not survive version upgrades. If your EPMM appliance is upgraded to a new version before 12.8.0.0 is released, you must reinstall the RPM script on the upgraded appliance. Maintain documentation of patch status across all EPMM instances to ensure consistent protection.

Investigate Potential Compromise: Review the Apache access log at /var/log/httpd/https-access_log for signs of exploitation using the provided regex pattern. Monitor for 404 HTTP response codes to the /mifs/c/aft store/fob/ and /mifs/c/app store/fob/ paths, which indicate attempted or successful exploitation. Ensure logs are forwarded to a SIEM solution for centralized monitoring.

Audit EPMM Configuration Changes: Examine your EPMM environment for unauthorized modifications including new or recently changed administrator accounts, alterations to authentication configurations such as SSO and LDAP settings, newly pushed applications for mobile devices, configuration changes to in-house applications, new or modified policies, and network configuration changes including VPN configurations pushed to mobile devices.

Implement Network Segmentation: Ensure EPMM appliances are properly segmented from critical network infrastructure. Limit network access to EPMM to only necessary systems and users, reducing the potential impact of a successful exploitation and limiting lateral movement opportunities.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Collection	T1005: Data from Local System	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
		T1588.005: Exploits

Patch Link

https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US

References

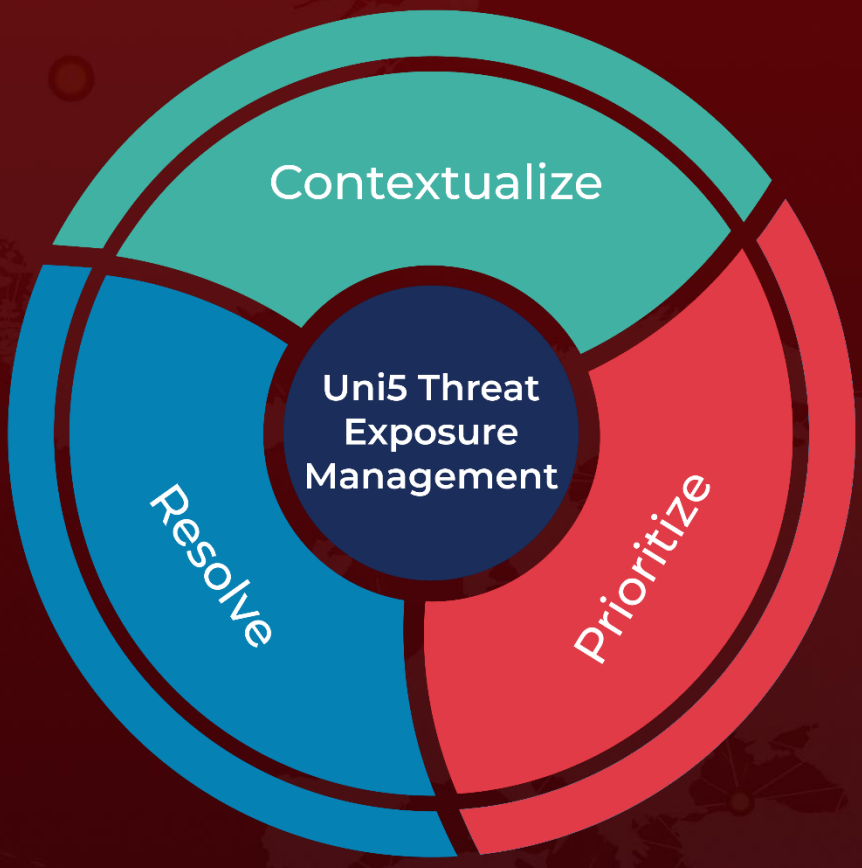
https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US

https://forums.ivanti.com/s/article/Analysis-Guidance-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 30, 2026 • 7:00 AM

More at www.hivepro.com