Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Ivanti Addresses Critical Zero-Day Vulnerabilities in EPMM Software

Date of Publication	Admiralty Code	TA Number
May 15, 2025	A1	TA2025150

Summary

First Seen: May 13, 2025
Affected Product: Ivanti Endpoint Manager Mobile
Impact: Ivanti has patched two critical zero-day vulnerabilities, CVE-2025-4427 and CVE-2025-4428, in its on-premises Endpoint Manager Mobile (EPMM) product after they were exploited in limited attacks. These vulnerabilities allow attackers to bypass authentication and remotely execute code, potentially giving them full control over affected systems. Organizations using Ivanti EPMM are strongly urged to act quickly and apply patches immediately.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-4427	Ivanti Endpoint Manager Mobile Authentication Bypass Vulnerability	Ivanti Endpoint Manager Mobile	✓	✗	✓
CVE-2025-4428	Ivanti Endpoint Manager Mobile Remote Code Execution Vulnerability	Ivanti Endpoint Manager Mobile	✓	✗	✓

Vulnerability Details

#1

Ivanti has recently addressed two critical zero-day vulnerabilities, CVE-2025-4427 and CVE-2025-4428, in its on-premises Endpoint Manager Mobile (EPMM) product, a widely used mobile device management and endpoint security solution for enterprises. These vulnerabilities, which stem from unnamed open-source libraries integrated into EPMM, have already been exploited in limited attacks.

#2

CVE-2025-4427 is an authentication bypass vulnerability that allows attackers to access protected resources without valid credentials. CVE-2025-4428 is a remote code execution (RCE) vulnerability that enables attackers to execute arbitrary code on the target system.

#3 When chained, these vulnerabilities allow unauthenticated attackers to achieve full remote code execution on vulnerable EPMM servers. In essence, attackers can bypass login mechanisms and immediately execute malicious code, leading to complete control over the target device or system.

#4 Ivanti has released patches for all affected versions-11.12.0.5, 12.3.0.2, 12.4.0.2, and 12.5.0.1-and strongly urges customers to update immediately. As additional protection, administrators are advised to restrict API access using Ivanti's Portal Access Control Lists (ACLs) or external web application firewalls (WAFs). Notably, these vulnerabilities do not impact Ivanti's cloud-hosted solutions, including Ivanti Neurons for MDM and Ivanti Sentry.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-4427	Ivanti Endpoint Manager Mobile: 11.12.0.4 and prior, 12.3.0.1 and prior, 12.4.0.1 and prior, 12.5.0.0 and prior	cpe:2.3:a:ivanti:endpoint_manager_mobile:*:*:*:*:*:*:*	CWE-288
CVE-2025-4428	Ivanti Endpoint Manager Mobile: 11.12.0.4 and prior, 12.3.0.1 and prior, 12.4.0.1 and prior, 12.5.0.0 and prior	cpe:2.3:a:ivanti:endpoint_manager_mobile:*:*:*:*:*:*:*	CWE-94

Recommendations

Apply Patches: Upgrade to the latest patched versions of Ivanti EPMM (11.12.0.5, 12.3.0.2, 12.4.0.2, or 12.5.0.1) as released by Ivanti. This is the most effective way to eliminate the vulnerabilities. Prioritize patching for any EPMM servers that are exposed to the internet or handle sensitive data.

Restrict API Access: Limit access to the EPMM API by configuring Ivanti’s Portal Access Control Lists (ACLs) to allow only trusted IP addresses or management networks. Deploy a Web Application Firewall (WAF) in front of the EPMM server to block suspicious or unauthorized API requests.

Apply RPM-Based Mitigation: If immediate patching is not possible, Ivanti provides an RPM file as an interim mitigation. Administrators can obtain this RPM by contacting Ivanti Support. Once acquired, the RPM should be installed via SSH access to the EPMM system, followed by a system reboot to apply the changes. This approach offers a temporary safeguard until full patching can be completed.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0004** Privilege Escalation
TA0006 Credential Access	**T1588** Obtain Capabilities	**T1588.005** Exploits	**T1059** Command and Scripting Interpreter
T1203 Exploitation for Client Execution	**T1190** Exploit Public-Facing Application	**T1068** Exploitation for Privilege Escalation	**T1588.006** Vulnerabilities

Patch Details

Upgrade Ivanti EPMM to versions 11.12.0.5, 12.3.0.2, 12.4.0.2, and 12.5.0.1 or later versions to fix the vulnerabilities CVE-2025-4427 and CVE-2025-4428.

Link:
https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM

References

https://cert.europa.eu/publications/security-advisories/2025-018/

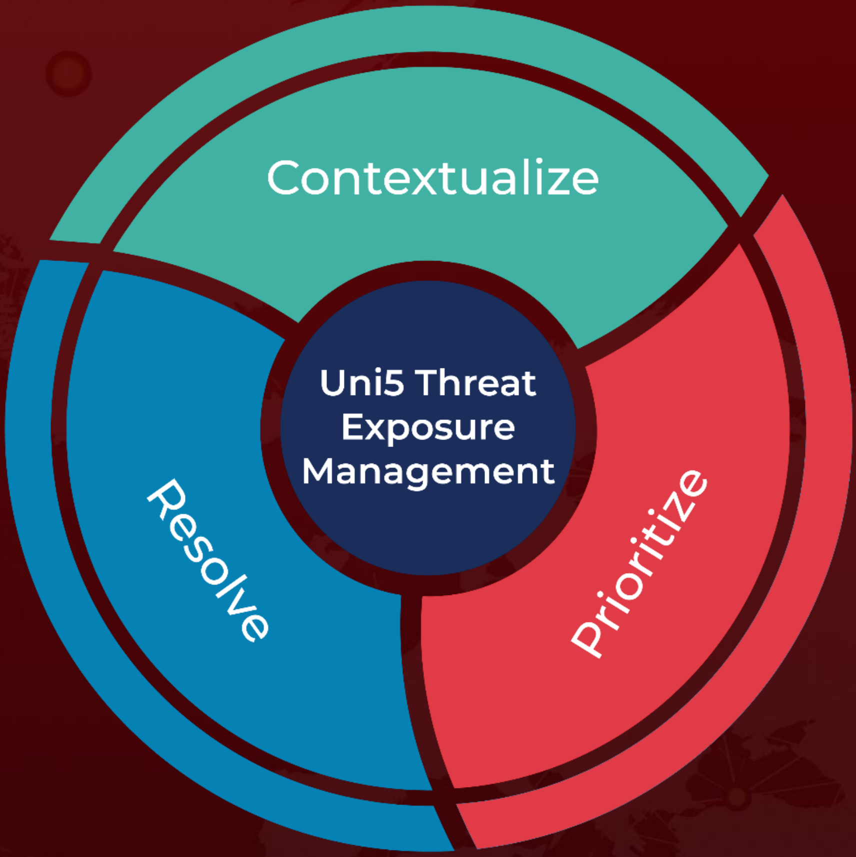
https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/multiple-vulnerabilities-in-ivanti-endpoint-manager-mobile

https://www.jpcert.or.jp/at/2025/at250011.html

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

May 15, 2025 • 6:30 AM

More at www.hivepro.com