Security Advisory 2024-050

Multiple Vulnerabilities in Ivanti EPMM

May 22, 2024 — v1.0

TLP:CLEAR

History:

- *22/05/2024 — v1.0 – Initial publication*

Summary

On May 15, 2024, Ivanti released a security advisory addressing multiple vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM), formally known as MobileIron. An attacker could exploit these flaws to execute arbitrary commands on the appliance.

It is strongly advised updating affected systems to the latest versions to mitigate these risks.

Technical Details

The vulnerability **CVE-2024-22026**, with a CVSS score of 6.7 is a local privilege escalation vulnerability allowing an authenticated user to execute arbitrary commands with root privileges by crafting and delivering a malicious RPM package. [1,2,3]

The vulnerabilities **CVE-2023-46806** and **CVE-2023-46807**, both with a CVSS score of 6.7, are SQL Injection vulnerabilities in the web component of EPMM which allows an authenticated user with appropriate privilege to access or modify data in the underlying database. [1]

Affected Products

- Ivanti Endpoint Manager Mobile (EPMM) versions 12.0 and earlier.

Recommendations

It is strongly recommended to update affected devices to version 12.1.0.0 or later. [2]

References

[1] https://www.ivanti.com/blog/may-security-update

[2] https://forums.ivanti.com/s/article/KB-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-May-2024?language=en_US

[3] https://www.redlinecybersecurity.com/blog/exploiting-cve-2024-22026-rooting-ivanti-epmm-mobileiron-core