UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0335

IVANTI PATCHES ZERO-DAY VULNERABILITY

DATE ISSUED: 02nd August 2023

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Ivanti has patched a critical zero-day vulnerability in its Endpoint Manager Mobile software which is formerly known as MobileIron Core. This vulnerability is leveraged to breach the IT systems by enabling an authenticated attacker to perform arbitrary file writes to the EPMM server.

BREAKDOWN

Ivanti EPMM is a mobile management software engine that enables IT administrators to set policies for mobile devices, applications, and content. The critical vulnerability in the EPMM server tracked as CVE-2023-35081 can be used in conjunction with CVE-2023-35078 which could allow an unauthenticated user to bypass administrator authentications and Access Control Lists restrictions. If the vulnerability is successfully exploited, it enables an attacker to write harmful files to the appliance. This, in turn, grants the malicious actor the ability to execute operating system commands on the appliance, all while assuming the identity of the tomcat user. The affected EPMM versions are 11.10 prior to 11.10.0.3, 11.9 prior to 11.9.1.2, 11.8 prior to 11.8.1.2, and EPMM Unsupported and End of Life versions.

REMEDIATION STEPS

- Apply appropriate updates provided by Ivanti to vulnerable systems immediately after appropriate testing.
- Employ robust network monitoring and intrusion detection systems to detect suspicious activities or anomalous behaviours.
- Use a Web Application Firewall (WAF) to protect web applications and filter out potentially malicious traffic and requests.
- Practice the Principle of Least Privilege and strong access controls on all systems and services to lower the risk of attacks.

REFERENCES & RESOURCES

Bleeping Computer https://www.bleepingcomputer.com/news/security/ivanti-patches-new-zero-day-exploited-in-norwegian-govt-attacks/

MS-ISAC Advisory https://www.cisecurity.org/advisory/a-vulnerability-in-ivanti-endpoint-manager-mobile-could-allow-for-arbitrary-code-execution_2023-087