Security Advisory 2023-055

High Vulnerability in Endpoint Manager Mobile (MobileIron Core)

July 31, 2023 — v1.0

TLP:CLEAR

History:

- *31/07/2023 — v1.0 – Initial publication*

Summary

On July 28, 2023, US-based IT software company Ivanti disclosed a Remote File Write vulnerability in its Endpoint Manager Mobile (EPMM) software, previously known as MobileIron Core [1].

The vulnerability tracked as **CVE-2023-35081** with as CVSS score of 7.2 out of 10, is **actively exploited** and allows an attacker to create, modify, or delete files on a victim's system remotely [1]. Ivanti has released security patches [2] addressing this vulnerability.

Technical Details

CVE-2023-35081 enables an authenticated administrator to perform arbitrary file writes to the EPMM server. This vulnerability can be used in conjunction with **CVE-2023-35078** [3], bypassing administrator authentication and ACLs restrictions (if applicable).

Successful exploitation can be used to write malicious files to the appliance, ultimately allowing a malicious actor to execute OS commands on the appliance as the tomcat user.

Affected Products

Ivanti reports the vulnerability impacts all supported versions of Ivanti Endpoint Manager Mobile (EPMM) – Version 11.4 releases 11.10, 11.9 and 11.8.

Note that **older versions/releases are also at risk**.

Recommendations

CERT-EU strongly recommends reviewing Ivanti's security advisory [2] and upgrading affected systems to avoid potential exploitation of this vulnerability.

References

[1] https://www.mnemonic.io/resources/blog/threat-advisory-remote-file-write-vulnerability-in-ivanti-epmm/

[2] https://forums.ivanti.com/s/article/KB-Arbitrary-File-Write-CVE-2023-35081?language=en_US

[3] https://www.cert.europa.eu/static/security-advisories/CERT-EU-SA2023-053.pdf