Security Advisory 2023-053

Critical vulnerability in Endpoint Manager Mobile (EPMM)

July 25, 2023 — v1.0

TLP:CLEAR

History:

- *25/07/2023 — v1.0 – Initial publication*

Summary

On July 24, 2023, US-based IT software company Ivanti disclosed a zero-day authentication bypass vulnerability in its Endpoint Manager Mobile (EPMM) software, previously known as MobileIron Core [1].

The vulnerability tracked as **CVE-2023-35078** with as CVSS score of 10 out of 10, is **actively exploited** and allows unauthorised users to access restricted functionality or resources of the application [1]. Ivanti has released security patches [2] addressing this vulnerability.

Technical Details

The authentication bypass vulnerability in Ivanti's EPMM software, i.e., **CVE-2023-35078**, grants unauthorised users access to restricted parts of the application without requiring appropriate authentication. By exploiting this vulnerability, an unauthorised, remote actor could access users personally identifiable information and make limited changes to the server [1].

It is important to note that all supported versions of the software, including versions 11.10, 11.9, and 11.8, are impacted by this vulnerability. Older versions or releases of the software are also at risk.

Despite not publicly acknowledging that the vulnerability was actively exploited, Ivanti has received credible information indicating exploitation against a small number of customers [1].

Affected Products

This vulnerability affects supported EPMM versions 11.10, 11.9, and 11.8. Unsupported older versions are also affected.

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.bleepingcomputer.com/news/security/ivanti-patches-mobileiron-zero-day-bug-exploited-in-attacks/

[2] https://forums.ivanti.com/s/article/CVE-2023-35078-Remote-unauthenticated-API-access-vulnerability?language=en_US