Security Advisory 2023-088

High Vulnerabilities in Ivanti Endpoint Manager Mobile

November 13, 2023 — v1.0

TLP:CLEAR

History:

- *13/11/2023 — v1.0 – Initial publication*

Summary

On November 9 2023, Ivanti disclosed two vulnerabilities, `CVE-2023-39335` and `CVE-2023-39337`, affecting all versions of Endpoint Manager Mobile (formerly MobileIron Core).

The vulnerabilities can be chained to allow an unauthenticated user to access resources behind Sentry [1].

Technical Details

`CVE-2023-39335`, with a CVSS score of 8.5 this vulnerability enables an authenticated user (enrolled device) to enrol a device for another EPMM user. The attacker must obtain additional information, such as by monitoring TLS traffic, to identify the user they would want to impersonate.

`CVE-2023-39337`, with a CVSS score of 6.8, this vulnerability enables an authenticated user (enrolled device) to obtain a valid certificate for another EPMM user. Like the previous vulnerability, the attacker must obtain additional information, such as by monitoring TLS traffic, to identify the user they would want to impersonate.

Affected Products

These vulnerabilities impact all supported versions of the products – EPMM Versions 11.10, 11.9 and 11.8 and Sentry Versions 9.18. 9.17 and 9.16. Older versions/releases are also at risk.

Recommendations

For both vulnerabilities, Ivanti released a patch included in the following EPMM (Core) releases. 11.10.0.4, 11.11.0.2, 11.12.0.0.

CERT-EU recommends immediately applying updates provided by Ivanti to vulnerable systems.

References

[1] https://www.ivanti.com/blog/ivanti-epmm-cve-2023-39335-39337

[2] https://forums.ivanti.com/s/article/CVE-2023-39337?language=en_US

[3] https://forums.ivanti.com/s/article/CVE-2023-39335?language=en_US