Security Advisory 2023-056

Critical Vulnerability in Endpoint Manager Mobile (MobileIron Core)

August 8, 2023 — v1.0

TLP:CLEAR

History:

- *08/08/2023 — v1.0 – Initial publication*

Summary

On August 2, Ivanti disclosed a Remote Unauthenticated API Access Vulnerability affecting EPMM (MobileIron Core) running outdated versions (11.2 and below) [1,2]. On August 7, Ivanti added more recent and supported versions on the list of affected products.

The vulnerability tracked as **CVE-2023-35082** with as CVSS score of 10 out of 10, is **actively exploited** and allows an unauthorised, remote actor to potentially access users personally identifiable information and make limited changes to the server. [1]. Ivanti has released security patches [1] addressing this vulnerability. This vulnerability is different from **CVE-2023-35078** [3] and **CVE-2023-35081** [4].

Technical Details

CVE-2023-35082 enables an unauthorised, remote actor to potentially access users personally identifiable information and make limited changes to the server by accessing non-restricted API endpoints, namely `/mifs/asfV3/api/v2/*`.

Affected Products

Ivanti reports the vulnerability impacts the following versions of Ivanti Endpoint Manager Mobile (EPMM):

- Endpoint Manager Mobile 11.10
- Endpoint Manager Mobile 11.9
- Endpoint Manager Mobile 11.8
- MobileIron Core 11.7 and below

Note that **older versions/releases are also at risk** (MobileIron Core 11.2 has been out of support since March 15, 2022).

Recommendations

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

CERT-EU also recommends reviewing the http access logs (`http-access_log`), available in the `/var/log/httpd/` folder in order to check for requests targeting the API endpoint containing `/mifs/asfV3/api/v2/` in the path. Requests with an HTTP response code of 200 would indicate successful attempts while blocked exploitation attempts will show an HTTP response code of either 401 or 403.

References

[1] https://forums.ivanti.com/s/article/CVE-2023-35082-Remote-Unauthenticated-API-Access-Vulnerability-in-MobileIron-Core-11-2-and-older?language=en_US

[2] https://www.rapid7.com/blog/post/2023/08/02/cve-2023-35082-mobileiron-core-unauthenticated-api-access-vulnerability/

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

[4] https://www.cert.europa.eu/static/security-advisories/CERT-EU-SA2023-055.pdf