CERT-EU

Security Advisory 2024-072

Vulnerabilities in Ivanti EPMM

July 22, 2024 — v1.0

TLP:CLEAR

History:

- *22/07/2024 — v1.0 – Initial publication*

Summary

On July 17, 2024, Ivanti released a security advisory addressing several vulnerabilities in its EPMM solution (formerly known as MobileIron) [1,2]. These vulnerabilities could lead to remote code execution, authentication bypass, and sensitive information leakage.

It is recommended updating as soon as possible.

Technical Details

The vulnerability **CVE-2024-36130**, with a CVSS score of 9.8, is a flaw (insufficient authorisation checks) in the web component of EPMM that would allow an unauthorised attacker within the network to execute arbitrary commands on the underlying operating system of the appliance [1].

The vulnerability **CVE-2024-36131**, with a CVSS score of 8.8, is a flaw (insecure deserialisation) in the web component of EPMM that would allow an authenticated remote attacker to execute arbitrary commands on the underlying operating system of the appliance [1].

The vulnerability **CVE-2024-36132**, with a CVSS score of 8.2, is a flaw (insufficient checks) in the authentication controls of EPMM that would allow a remote attacker to bypass authentication and access sensitive resources [1].

The vulnerability **CVE-2024-34788**, with a CVSS score of 5.3, is a flaw (improper authentication) in the web component of EPMM that would allow a remote malicious user to access potentially sensitive information [1].

Affected Products

These vulnerabilities affect EPMM versions prior to `12.1.0.1` [1].

Recommendations

CERT-EU recommends updating affected devices to the latest version as soon as possible [1].

References

[1] https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-for-Mobile-EPMM-July-2024?language=en_US

[2] https://www.securityweek.com/ivanti-issues-hotfix-for-high-severity-endpoint-manager-vulnerability/