Overall Rating - Critical

BRITISH COLUMBIA

****

Number: AL23-011
Date: July 25, 2023

Title

Threat Actors Exploiting Ivanti Endpoint Manager Mobile CVE-2023-35078

Audience

This Alert is intended for IT professionals and managers of notified organizations.

Purpose

An Alert is used to raise awareness of a recently identified cyber threat that may impact cyber information assets, and to provide additional detection and mitigation advice to recipients.
The Canadian Centre for Cyber Security ("Cyber Centre") is also available to provide additional assistance regarding the content of this Alert to recipients as requested.

Details

On July 24, 2023, Ivanti published an article [1] highlighting a remotely exploitable vulnerability (CVE-2023-35078) in Ivanti Endpoint Manager Mobile (EPMM) (formerly MobileIron Core). Ivanti has stated that exploitation of this vulnerability enables an unauthorized, remote (internet-facing) actor to potentially access users' personally identifiable information and make limited changes to the server. CISA has since published an Alert which further states that this vulnerability may also result in other configuration changes, including the creation of an EPMM administrative account that can make further changes to a vulnerable system. [2] Ivanti additionally reported that this vulnerability has been exploited, and Norway's National Security Authority and Departments' Security and Service Organization have stated publicly [3] they have been affected by this zero-day vulnerability.

On July 25, 2023, the Cyber Centre published AV23-434 [4] highlighting the vulnerability in Ivanti Endpoint Manager Mobile (EPMM). The advisory raised awareness that a vulnerability exists and that it had been exploited. The Cyber Centre has assessed that there are a number of potentially affected devices within Canada.

Recommendations

The Cyber Centre recommends that any organizations who use these devices, to ensure that they are patched as soon as possible.

Additional guidance is available in the Cyber Centre's Top 10 IT security actions to protect Internet connected networks and information (ITSM.00.089) [5]. These publications are based on analysis of cyber threat trends to help minimize intrusions or the impacts of a successful cyber intrusion.

References

[0] CVE-2023-35078

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

[2] CISA - Ivanti Releases Security Updates for Endpoint Manager Mobile (EPMM) CVE-2023-35078:
https://www.cisa.gov/news-events/alerts/2023/07/24/ivanti-releases-security-updates-endpoint-manager-mobile-epmm-cve-2023-35078

[3] Norwegian Statement:
https://nsm.no/aktuelt/nulldagssarbarhet-i-ivanti-endpoint-manager-mobileiron-core (In Norwegian only)

[4] CCCS AV23-434 Ivanti security advisory:
https://www.cyber.gc.ca/en/alerts-advisories/ivanti-security-advisory-av23-434

[5] Top 10 IT security actions to protect Internet connected networks and information (ITSM.00.089):
https://www.cyber.gc.ca/en/guidance/top-10-it-security-actions-protect-internet-connected-networks-and-information-itsm10089

****