Security Advisory 2025-018

Zero-Day Vulnerabilities in Ivanti EPMM

2025-05-15 — v1.2

TLP:CLEAR

History:

- *13/05/2025 — v1.0 – Initial publication*
- *14/05/2025 — v1.1 – Fix a typo*
- *15/05/2025 — v1.2 – Add information from WatchTowr and detection opportunities.*

Summary

On May 13, 2025, Ivanti released a security advisory addressing two zero-day vulnerabilities in their EPMM products. An attacker could chain those vulnerabilities to achieve unauthenticated remote code execution on the vulnerable device. These vulnerabilities have been exploited in a limited number of cases [1].

[New] The analysis conducted by WatchTowr [3] provides significantly more information than the advisory issued by Ivanti in two key aspects:

- WatchTowr attributes the vulnerabilities to code owned by Ivanti, whereas Ivanti asserts that they are related to third-party libraries.
- Additionally, WatchTowr questions the validity of the reported authentication bypass vulnerability, disagreeing with Ivanti's assessment.

CERT-EU strongly recommends applying the update as soon as possible, prioritising Internet facing devices.

Technical Details

The vulnerability **CVE-2025-4427**, with a CVSS score of 5.3, is an authentication bypass in Ivanti Endpoint Manager Mobile (EPMM) allowing attackers to access protected resources without proper credentials.

The vulnerability **CVE-2025-4428**, with a CVSS score of 7.2, is a remote code execution vulnerability in Ivanti Endpoint Manager Mobile (EPMM) allowing attackers to execute arbitrary code on the target system.

These two vulnerabilities could be chained to achieve unauthenticated remote code execution on the vulnerable device.

[New] WatchTowr's further examination of the EPMM fix suggests that assigning two separate CVEs may be unnecessary [3]. The application's design appears to allow for the exploitation of both vulnerabilities without requiring a valid login, implying that they could be considered as a single, more severe vulnerability - potentially critical in nature.

Affected Products

Ivanti's Endpoint Manager Mobile (EPMM) versions 12.5.0.0 and prior are affected by these vulnerabilities.

Recommendations

CERT-EU strongly recommends applying the update as soon as possible, prioritising Internet facing devices.

Workaround

If it is not possible to update vulnerable assets immediately, it is possible to apply the following mitigation measures:

1. Customers can mitigate the threat by following best practice guidance of filtering access to the API using either the build in Portal ACLs functionality or an external WAF [2].
2. An RPM file can be provided by Ivanti with a hot-fix mitigation, if customers need an alternative option. Customers will need to open a Support Case to receive the RPM file, and follow the step-by-step guide provided by Ivanti [1].

[New] Detection opportunities

The best detection opportunity to look for exploitation of this vulnerability is to search the HTTP logs for unexpected requests against the vulnerable API endpoints:

```
GET /mifs/rs/api/v2/featureusage?format=<USER_INPUT> HTTP/1.1
GET /mifs/rs/api/v2/featureusage_history?format=<USER_INPUT> HTTP/1.1
```

Where `<USER_INPUT>` is not one of the expected values provided in the documentation (i.e. `csv` or `json`).

References

[1] https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM

[2] https://help.ivanti.com/mi/help/en_us/core/12.x/sys/CoreSystemManager/Access_Control_Lists__Po.htm

[3] https://labs.watchtowr.com/expression-payloads-meet-mayhem-cve-2025-4427-and-cve-2025-4428/?123

[4] https://docs.jboss.org/hibernate/stable/validator/reference/en-US/html_single/?v=6.1&ref=labs.watchtowr.com#el-features