January 5, 2024

Overall rating: Critical

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Ivanti a publié un bulletin de sécurité visant à corriger une vulnérabilité critique liée aux produits suivants :

- Ivanti EPM 2021 – versions antérieures à SU5;
- Ivanti EPM 2022 – versions antérieures à SU5.

Technical Details

If exploited, an attacker with access to the internal network can leverage an unspecified SQL injection to execute arbitrary SQL queries and retrieve output without the need for authentication. This can then allow the attacker control over machines running the EPM agent. When the core server is configured to use SQL express, this might lead to RCE on the core server.

These vulnerabilities are rated as an overall **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-39336
- Ivanti Security Advisory - SA-2023-12-19-CVE-2023-39336 (en anglais seulement)
- Ivanti Security Advisories (en anglais seulement)