**Overall Rating - High**

BRITISH COLUMBIA

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

## Summary

The Vulnerability and Risk Management (VRM) Team is aware a vulnerability has been discovered in Ivanti Sentry, formerly known as MobileIron Sentry. This vulnerability impacts versions 9.18 and prior.

## Technical Details

Exploitation of this vulnerability enables an unauthenticated actor to access some sensitive APIs that are used to configure the Ivanti Sentry on the administrator portal (port 8443, commonly MICS). There is a low risk of exploitation for customers who do not expose port 8443 to the internet.

Successful exploitation can be used to change configuration, run system commands, or write files onto the system. Ivanti recommends that customers restrict access to MICS to internal management networks and not expose this to the internet.

This vulnerability is rated as a **High** 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-2023-38035
- https://forums.ivanti.com/s/article/CVE-2023-38035-API-Authentication-Bypass-on-Sentry-Administrator-Interface