April 22, 2024

Overall rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware OpenMetadata platform published a security advisory to address vulnerabilities in the following products:

- Affecting versions prior to 1.3.1

Technical Details

These vulnerabilities (CVE-2024-28255, CVE-2024-28847, CVE-2024-28253, CVE-2024-28848, CVE-2024-28254), affecting versions prior to 1.3.1, could be exploited by attackers to bypass authentication and achieve remote code execution. Since the beginning of April, we have observed exploitation of this vulnerability in Kubernetes environments.

Microsoft highly recommends customers to check clusters that run OpenMetadata workload and make sure that the image is up to date (version 1.3.1 or later)

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

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

References

- CVE-2024-28255 CVE-2024-28847 CVE-2024-28253 CVE-2024-28848 CVE-2024-28254
- Attackers exploiting new critical OpenMetadata vulnerabilities on Kubernetes clusters | Microsoft Security Blog