October 16, 2023

Overall Rating - High

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

Between October 9 and October 15, 2023, IBM published security advisories to address vulnerabilities in multiple products. Included were critical updates for the following:

- IBM Business Automation Manager Open Editions – versions 8.0.0 to 8.0.3
- IBM Db2 REST – versions 1.0.0.121-amd64 to 1.0.0.276-amd64
- IBM Engineering Lifecycle Optimization - Publishing – versions 7.0.1 and 7.0.2
- IBM Jazz Reporting Service – versions 7.0.1 and 7.0.2
- IBM Operations Analytics Predictive Insights – version 1.3.6
- IBM Process Mining – versions 1.14.0 and 1.14.1
- IBM QRadar SIEM – versions 7.5.0 to 7.5.0 UP6
- IBM QRadar User Case Manager App – versions 1.0 to 3.7.0
- IBM Robotic Process Automation for Cloud Pak – versions 21.0.0 to 21.0.7.8 and versions 23.0.0 to 23.0.9
- IBM Storage Protect for Virtual Environments: Data Protection for VMware – versions 8.1.0.0 to 8.1.14.0
- Red Hat Certified Ansible Collection for IBM Storage Virtualize – all versions

Technical Details

FasterXML jackson-databind is vulnerable to a denial of service, caused by a Java StackOverflow exception. By using a large depth of nested objects, a remote attacker could exploit this vulnerability to cause a denial of service.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **high** risk. A software update exists to address this risk.

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-2020-36518, CVE-2023-43642, CVE-2022-43680
- IBM Product Security Incident Response

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts