July 11, 2024

Overall Rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a VMware released a security advisory to address a vulnerability in the following product:

- VMware Aria Automation – versions 8.x
- VMware Cloud Foundation – versions 5.x and 4.x

Technical Details

VMware Aria Automation does not apply correct input validation which allows for SQL-injection in the product. VMware has evaluated the severity of this issue to be in the important severity range with a maximum CVSSv3 base score of 8.5.

Known Attack Vectors:

An authenticated malicious user could enter specially crafted SQL queries and perform unauthorised read/write operations in the database.

Resolution:

To remediate CVE-2024-22280 apply the patches listed in the 'Fixed Version' column of the 'Response Matrix' found below.

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 at VulnerabilityandRiskManagement@gov.bc.ca

References

- CVE-2024-22280
- VMware VMSA-2024-0017
- Security Advisories - VMware Cloud Foundation