July 4, 2024

Overall Rating: Medium

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of multiple VMware Cloud Director vulnerabilities. The vulnerability affects VMware Cloud Director Availability 4.x, VMware Cloud Director Object Storage Extension 2.x and 3.0 and VMware Cloud Director 10.5.x/10.4.x.

Technical Details

VMware Cloud Director Availability contains an HTML injection vulnerability. A malicious actor with network access to VMware Cloud Director Availability can craft malicious HTML tags to execute within replication tasks.

VMware Cloud Director Object Storage Extension contains an Insertion of Sensitive Information vulnerability. A malicious actor with adjacent access to web/proxy server logging may be able to obtain sensitive information from URLs that are logged.

VMware Cloud Director contains an Improper Privilege Management vulnerability. An authenticated tenant administrator for a given organization within VMware Cloud Director may be able to accidentally disable their organization leading to a Denial of Service for active sessions within their own organization's scope.

This vulnerability is rated as a **MEDIUM** 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 atVulnerabilityandRiskManagement@gov.bc.ca.

References

- CVE-2024-22277, CVE-2024-22276, CVE-2024-22272
- VMSA-2024-0016: VMware Cloud Director Availability addresses an HTML injection vulnerability (CVE-2024-22277)
- VMSA-2024-0015: VMware Cloud Director Object Storage Extension addresses an Insertion of Sensitive Information vulnerability (CVE-2024-22276)
- VMSA-2024-0014: VMware Cloud Director addresses an improper privilege management vulnerability (CVE-2024-22272)
- VRM Vulnerability Reports