June 19, 2024

Overall Rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

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

- VMware vCenter Server – versions 8.0 prior to 8.0 U2d, versions 8.0 prior to 8.0 U1e and versions 7.0 prior to 7.0 U3r
- VMware Cloud Foundation (vCenter Server) – versions 4.x and 5.x

Technical Details

The vCenter Server contains multiple heap-overflow vulnerabilities in the implementation of the DCERPC protocol. VMware has evaluated the severity of these issues to be in the Critical severity range with a maximum CVSSv3 base score of 9.8.

Known Attack Vectors:
A malicious actor with network access to vCenter Server may trigger these vulnerabilities by sending a specially crafted network packet potentially leading to remote code execution.

This vulnerability is rated as a **CRITICAL** 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-2024-37079, CVE-2024-37080, CVE-2024-37081
- VMSA-2024-0012:VMware vCenter Server updates address heap-overflow and privilege escalation vulnerabilities (CVE-2024-37079, CVE-2024-37080, CVE-2024-37081)
- Security Advisories - VMware Cloud Foundation
- VRM Vulnerability Reports