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 vulnerabilities in ESXi and vCenter Server. The vulnerability affects ESXi versions 7.0 and 8.0 and VMware Cloud Foundation 4.x and 5.x.

Technical Details

VMware ESXi contains an authentication bypass vulnerability. A malicious actor with sufficient Active Directory (AD) permissions can gain full access to an ESXi host that was previously configured to use AD for user management by re-creating the configured AD group ('ESXi Admins' by default) after it was deleted from AD.

VMware ESXi contains an out-of-bounds read vulnerability. A malicious actor with local administrative privileges on a virtual machine with an existing snapshot may trigger an out-of-bounds read leading to a denial-of-service condition of the host.

The vCenter Server contains a denial-of-service vulnerability. A malicious actor with network access to vCenter Server may create a denial-of-service condition.

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-2024-37085, CVE-2024-37086, CVE-2024-37087
- VMSA-2024-0013: VMware ESXi and vCenter Server updates address multiple security vulnerabilities (CVE-2024-37085, CVE-2024-37086, CVE-2024-37087)
- VRM Vulnerability Reports