July 31, 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 VMware published a security advisory to address critical vulnerabilities in the following products:

- VMware ESXi and vCenter Server

Technical Details

VMware ESXi contains an authentication bypass vulnerability. VMware has evaluated the severity of this issue to be in the Moderate severity range with a maximum CVSSv3 base score of 6.8..

Known Attack Vectors:
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 ('ESX Admins' by default) after it was deleted from AD.

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-2024-37085 CVE-2024-37086 CVE-2024-37087
- Support Content Notification - Support Portal - Broadcom support portal