May 22, 2024

Overall Rating - High

This notification is intended as an informational bulletin for technical audiences.

Summary

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

- VMware Cloud Foundation (ESXi) – multiple versions
- VMware Cloud Foundation (vCenter Server) – multiple versions
- VMware ESXi – versions 8.0 prior to ESXi80U2sb-23305545 and versions 7.0 prior to ESXi70U3sq-23794019
- VMware Fusion – versions prior to 13.5.1
- VMware vCenter Server – versions 8.0 prior to 8.0 U2b and versions 7.0 prior to 7.0 U3q
- VMware Workstation – versions prior to 17.5.1

Technical Details

The storage controllers on VMware ESXi, Workstation, and Fusion have out-of-bound read/write vulnerability. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 8.1.

Known Attack Vectors:

A malicious actor with access to a virtual machine with storage controllers enabled may exploit this issue to create a denial-of-service condition or execute code on the hypervisor from a virtual machine in conjunction with other issues.

.These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-22273 CVE-2024-22274 CVE-2024-22275
- VMSA-2024-0011:VMware ESXi, Workstation, Fusion and vCenter Server updates address multiple security vulnerabilities (CVE-2024-22273, CVE-2024-22274, CVE-2024-22275)
- Security Advisories - VMware Cloud Foundation