March 5, 2024

Overall rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended 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 – versions 4.x and 5.x
- VMware ESXi – versions 7.0 and 8.0
- VMware Fusion for MacOS – versions 13.x prior to 13.5.1
- VMware Workstation – versions 17.x prior to 17.5.1

Technical Details
VMware ESXi, Workstation, and Fusion contain a use-after-free vulnerability in the XHCI USB controller. VMware has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.3 for Workstation/Fusion and in the Important severity range with a maximum CVSSv3 base score of 8.4 for ESXi.

Known Attack Vectors

A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. On ESXi, the exploitation is contained within the VMX sandbox whereas, on Workstation and Fusion, this may lead to code execution on the machine where Workstation or Fusion is installed.

.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

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.

References

- CVE-2024-22252 CVE-2024-22253 CVE-2024-22254 CVE-2024-22255
- VMware Security Advisory - VMSA-2024-0006
- VMware Security Advisories