May 14, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

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

- VMware Fusion – versions 13.x prior to 13.5.2
- VMware Workstation – versions 17.x prior to 17.5.2

Technical Details

VMware Workstation and Fusion contain a use-after-free vulnerability in the vbluetooth device. VMware has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.3.

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.

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

- VMware Workstation and Fusion updates address multiple security vulnerabilities (CVE-2024-22267, CVE-2024-22268, CVE-2024-22269, CVE-2024-22270)
- Security Advisories - VMware Cloud Foundation