VMware Patches Severe Security Flaws in Workstation and Fusion Products

Date: 15th May 2024 | Severity: High

Summary

Broadcom-owned VMware on Tuesday published a security advisory to inform Workstation and Fusion customers that patches are available for vulnerabilities exploited earlier this year at the Pwn2Own hacking competition.

Attack Vectors

Multiple security flaws have been disclosed in VMware Workstation and Fusion products that could be exploited by threat actors to access sensitive information, trigger a denial-of-service (DoS) condition, and execute code under certain circumstances.

CVE-2024-22267 (CVSS score: 9.3) - A use-after-free vulnerability in the Bluetooth device that could be exploited by a malicious actor with local administrative privileges on a virtual machine to execute code as the virtual machine's VMX process running on the host.

CVE-2024-22268 (CVSS score: 7.1) - A heap buffer-overflow vulnerability in the Shader functionality that could be exploited by a malicious actor with non-administrative access to a virtual machine with 3D graphics enabled to create a DoS condition.

CVE-2024-22269 (CVSS score: 7.1) - An information disclosure vulnerability in the Bluetooth device that could be exploited by a malicious actor with local administrative privileges on a virtual machine to read privileged information contained in hypervisor memory from a virtual machine.

CVE-2024-22270 (CVSS score: 7.1) - An information disclosure vulnerability in the Host Guest File Sharing (HGFS) functionality that could be exploited by a malicious actor with local administrative privileges on a virtual machine to read privileged information contained in hypervisor memory from a virtual machine.

Indicator of compromise

INDICATOR TYPE	INDICATORS
CVE	CVE-2024-22267, CVE-2024-22268, CVE-2024-22269, CVE-2024-22270
Impact	The impact Workstation versions 17.x and Fusion versions 13.x, with fixes available in version 17.5.2 and 13.5.2, respectively.

Recommendation

- We strongly recommend that all installations running a version affected by the issues are upgraded to the latest version as soon as possible.
- Enable two factor authentication (2FA) which will deny malicious actors access to compromised accounts.

Note: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://thehackernews.com/2024/05/vmware-patches-severe-security-flaws-in.html
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24280
- https://www.securityweek.com/vmware-patches-vulnerabilities-exploited-at-pwn2own-2024/