Se han revelado múltiples deficiencias de seguridad en los productos VMware Workstation y Fusion que podrían ser aprovechadas por actores maliciosos para acceder a información confidencial, desencadenar una condición de denegación de servicio (DoS) y ejecutar código en ciertos escenarios.

Estas cuatro vulnerabilidades afectan a las versiones 17.x de Workstation y a las versiones 13.x de Fusion. Las soluciones ya están disponibles en las versiones 17.5.2 y 13.5.2, respectivamente, según informó el proveedor de servicios de virtualización, propiedad de Broadcom.

Una breve sinopsis de cada fallo se detalla a continuación:

- CVE-2024-22267 (puntuación CVSS: 9.3) – Una debilidad de liberación tras el uso en el dispositivo Bluetooth, que podría ser aprovechada por un actor malicioso con privilegios administrativos locales en una máquina virtual para ejecutar código como el proceso VMX de la máquina virtual en el host.
- CVE-2024-22268 (puntuación CVSS: 7.1) – Un fallo de desbordamiento de búfer en la funcionalidad Shader que podría ser explotado por un atacante con acceso no administrativo a una máquina virtual con gráficos 3D activados para causar una condición de DoS.
- CVE-2024-22269 (puntuación CVSS: 7.1) – Una debilidad de divulgación de información en el dispositivo Bluetooth que podría ser aprovechada por un atacante malicioso con privilegios administrativos locales en una máquina virtual para leer datos privilegiados contenidos en la memoria del hipervisor de la máquina virtual.
- CVE-2024-22270 (puntuación CVSS: 7.1) – Una debilidad de divulgación de información en la funcionalidad de Compartir Archivos entre Anfitrión y Huésped (HGFS) que podría ser explotada por un atacante con privilegios administrativos locales en una máquina virtual para acceder a datos privilegiados contenidos en la memoria del hipervisor desde una máquina virtual.

Como medidas provisionales hasta que se implementen los parches, se recomienda a los usuarios desactivar el soporte Bluetooth en la máquina virtual y deshabilitar la función de

aceleración 3D. No hay soluciones que aborden CVE-2024-22270, aparte de actualizar a la versión más reciente.

Es importante señalar que CVE-2024-22267, CVE-2024-22269 y CVE-2024-22270 fueron inicialmente demostrados por STAR Labs SG y Theori en el concurso de hacking Pwn2Own celebrado en Vancouver a principios de marzo.

Este aviso llega más de dos meses después de que la compañía lanzara parches para abordar cuatro fallas de seguridad que afectaban a ESXi, Workstation y Fusion, incluyendo dos vulnerabilidades críticas (CVE-2024-22252 y CVE-2024-22253, puntuaciones CVSS: 9.3/8.4) que podrían conducir a la ejecución de código.