VMware ha lanzado actualizaciones para abordar cuatro vulnerabilidades de seguridad que afectan a ESXi, Workstation y Fusion, incluyendo dos fallos críticos que podrían resultar en la ejecución de código.

Identificadas como CVE-2024-22252 y CVE-2024-22253, estas vulnerabilidades se han caracterizado como defectos de *«uso después de liberación»* en el controlador USB XHCI. Estas presentan un puntaje CVSS de 9.3 para Workstation y Fusion, y de 8.4 para sistemas ESXi.

> Según la nueva advertencia de la compañía, *«Un actor malintencionado con privilegios administrativos locales en una máquina virtual puede aprovechar este problema para ejecutar código en el proceso VMX de la máquina virtual que se ejecuta en el host».*
>
> *«En el caso de ESXi, la explotación está contenida dentro del sandbox VMX, mientras que en Workstation y Fusion, esto podría llevar a la ejecución de código en la máquina donde está instalado Workstation o Fusion».*

Varios investigadores de seguridad asociados con el Ant Group Light-Year Security Lab y QiAnXin han sido reconocidos por descubrir e informar de manera independiente sobre el CVE-2024-22252. Los investigadores de seguridad VictorV y Wei han sido mencionados por reportar el CVE-2024-22253.

El proveedor de servicios de virtualización, propiedad de Broadcom, también ha corregido otras dos deficiencias:

- CVE-2024-22254 (puntaje CVSS: 7.9): una vulnerabilidad de escritura fuera de límites en ESXi que un actor malintencionado con privilegios dentro del proceso VMX podría explotar para eludir el sandbox.
- CVE-2024-22255 (puntaje CVSS: 7.1): una vulnerabilidad de divulgación de

información en el controlador USB UHCI que un atacante con acceso administrativo a una máquina virtual podría explotar para filtrar memoria del proceso vmx.

Estas problemáticas se han abordado en las siguientes versiones, incluso aquellas que han llegado al final de su ciclo de vida debido a la gravedad de estos problemas:

- ESXi 6.5 – 6.5U3v
- ESXi 6.7 – 6.7U3u
- ESXi 7.0 – ESXi70U3p-23307199
- ESXi 8.0 – ESXi80U2sb-23305545 y ESXi80U1d-23299997
- VMware Cloud Foundation (VCF) 3.x
- Workstation 17.x – 17.5.1
- Fusion 13.x (macOS) – 13.5.1

Como medida temporal hasta que se pueda implementar un parche, se insta a los clientes a eliminar todos los controladores USB de la máquina virtual. La compañía también señala que *«los dispositivos USB virtuales/emulados, como el stick o dongle USB virtual de VMware, no estarán disponibles para su uso en la máquina virtual».* Mientras tanto, los dispositivos predeterminados de teclado/ratón como dispositivos de entrada no se ven afectados, ya que, por defecto, no están conectados a través del protocolo USB, sino que cuentan con un controlador que realiza la emulación de dispositivo de software en el sistema operativo invitado.