BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-07
Fecha de publicación: 07/03/2024
Tema: Multiple vulnerabilidades reportadas en productos VMware.
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- VMware ESXi
- VMware Workstation Pro / Player (Workstation)
- VMware Fusion Pro / Fusion (Fusion)
- VMware Cloud Foundation (Cloud Foundation)

Descripción:

Se ha reportado múltiples vulnerabilidades en productos VMware, identificadas como CVE-2024-22252 con CVSSv3 de 9.3, CVE-2024-22253 con CVSSv3 de 9.3, CVE-2024-22254 con CVSSv3 de 7.9 y CVE-2024-22255 con CVSSv3 de 7.1. Las vulnerabilidades individuales documentadas en este reporte para VMware ESXi tienen una gravedad Alta, pero la combinación de estas vulnerabildiade dará como resultado una gravedad Crítica.

CVE-2024-22252: Vulnerabilidad de uso después de la liberación (Use-after-free) de memoria que afecta al controlador USB XHCI. El proveedor ha evaluado la gravedad de este problema en el rango de gravedad Crítico con una puntuación base CVSSv3 máxima de 9,3 para Workstation/Fusion y 8.4 para ESXi.

CVE-2024-22253: Vulnerabilidad de uso después de la liberación (Use-after-free) de memoria en el controlador USB UHCI. El proveedor ha evaluado la gravedad de este problema en el rango de gravedad Crítico con una puntuación base CVSSv3 máxima de 9,3 para Workstation/Fusion y 8.4 para ESXi.

CVE-2024-22254: Vulnerabilidad de escritura fuera de límites (Out-of-bounds) de ESXi, se ha asignado un CVSSv3 máxima de 7,9.

CVE-2024-22255: Vulnerabilidad de divulgación de información en el controlador USB UHCI, se ha asignado un CVSSv3 máxima de 7.1.

Impacto

Un actor malintencionado con privilegios administrativos locales en una máquina virtual puede aprovechar este problema para ejecutar código como el proceso VMX de la máquina virtual que se ejecuta en el host. En ESXi, la explotación está contenida dentro del entorno limitado de VMX, mientras que, en Workstation y Fusion, esto puede provocar la ejecución de código en la máquina donde está instalado Workstation o Fusion.

Solución

Se recomienda actualizar los dispositivos VMware con ESXi/Workstation/Fusion a las versiones parcheadas:

Version	Solución
ESXi 8.0	ESXi80U2sb-23305545
ESXi 8.0 [2]	ESXi80U1d-23299997
ESXi 7.0	ESXi70U3p-23307199
Workstation 17.x	Actualizar a la version 17.5.1
Fusion 13.x para MacOS	Actualizar a la version 13.5.1

Para más información sobre las versiones vulnerables puede consultar el reporte oficial aquí.

Código de campo cambiado

Mitigación

En caso de imposibilidad de aplicar el parche de manera inmediata, una mitigación La es la eliminación de todos los controladores USB de la máquina virtual. Como resultado, la funcionalidad de paso USB no estará disponible.

Eliminó: solución

Eliminó: r

Además, los dispositivos USB virtuales/emulados, como la memoria USB o el dongle virtual de VMware, no estarán disponibles para que los utilice la máquina virtual. Por el contrario, el teclado/ratón predeterminado como dispositivo de entrada no se ve afectado ya que, de forma predeterminada, no están conectados a través del protocolo USB, pero tienen un controlador que emula el dispositivo de software en el sistema operativo invitado.

Para mas información puede consultar la propuesta de mitigación oficial del fabricante aqui.

Código de campo cambiado

Información adicional:

- https://www.vmware.com/security/advisories/VMSA-2024-0006.html
- https://www.cisa.gov/news-events/alerts/2024/03/06/vmware-releases-security-advisory-multiple-products
- https://kb.vmware.com/s/article/96682

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com