Vulnerabilidades críticas en VMware ESXi, Workstation y Fusion

CYBERZAINTZA-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que la Agencia de Ciberseguridad Vasca considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso la Agencia de Ciberseguridad Vasca puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de la Agencia de Ciberseguridad Vasca como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de la Agencia de Ciberseguridad Vasca. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

1. Resumen ejecutivo

VMware ha publicado un aviso de seguridad relativo a **4 vulnerabilidades** de **severidad crítica,** con los identificadores CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255, que afectan a los productos **VMware ESXi, Workstation y Fusion.** Estos errores producen condiciones Use-After-Free, escritura fuera de límites y de **divulgación de información**, suponiendo, las de más severidad, una amenaza de alta gravedad con impacto en la confidencialidad, integridad y disponibilidad de los sistemas que se vean afectados.

El fabricante ya ha publicado las actualizaciones y medidas de mitigación correspondientes, corrigiendo de esta manera los fallos destacados. Por lo que, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

2. Recursos afectados

- VMware ESXi versiones 7.0 y 8.0.
- VMware Workstation Pro / Player versiones 17.x.
- VMware Fusion Pro / Fusion versiones 13.x.
- VMware Cloud Foundation versiones 5.x/4.x.

3. Análisis técnico

Los detalles de las vulnerabilidades tratadas en este aviso son los siguientes:

CVE-2024-22252: vulnerabilidad Use-After-Free en VMware ESXi, Workstation y Fusion en el controlador USB XHCI. Un actor malicioso con privilegios administrativos locales en una máquina virtual puede aprovechar este problema para ejecutar código como el proceso VMX de la máquina virtual en ejecución en el host. En ESXi, la explotación está contenida dentro del sandbox de VMX, mientras que en Workstation y Fusion, esto puede llevar a la ejecución de código en la máquina donde está instalado Workstation o Fusion.

La métrica de evaluación de las vulnerabilidades se compone de:

CVSS Base: **8.4**

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque**: Local
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2024-22253: vulnerabilidad Use-After-Free en VMware ESXi, Workstation y Fusion en el controlador USB XHCI. 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 en ejecución en el host. En ESXi, la explotación está contenida dentro del sandbox de VMX, mientras que en Workstation y Fusion, esto puede llevar a la ejecución de código en la máquina donde está instalado Workstation o Fusion.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **8.4**

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque**: Local
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**

- **Disponibilidad: Alta**

CVE-2024-22254: vulnerabilidad de escritura fuera de límites en VMware ESXi. Un actor malintencionado con privilegios dentro del proceso VMX puede desencadenar una escritura fuera de límites que conduzca a un escape del sandbox.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **7.9**

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N

- **Vector de ataque**: Local
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos:** Altos
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad:** Ninguna

CVE-2024-22255: vulnerabilidad de divulgación de información en VMware ESXi, Workstation y Fusion en el controlador USB UHCI. Un actor malintencionado con acceso administrativo a una máquina virtual podría aprovechar este problema para filtrar memoria desde el proceso vmx.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **7.1**

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

- **Vector de ataque**: Local
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad:** Ninguna
- **Disponibilidad:** Ninguna

4. Mitigación / Solución

Como es habitual, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

En respuesta a estas vulnerabilidades, VMware recomienda a sus clientes que actualicen a las versiones corregidas, que son las siguientes:

- Para ESXi 8.0 actualizar a ESXi80U2sb-23305545.
- Para ESXi 8.0 [2] actualizar a ESXi80U1d-23299997.
- Para ESXi 7.0 actualizar a ESXi70U3p-23307199.
- Para Workstation 17.x actualiza a la versión 17.5.1.
- Para Fusion 13.x actualiza a la versión 13.5.1.
- Para Cloud Foundation (ESXi) 5.x/4.x actualizar a KB88287.

Adicionalmente, para todas las vulnerabilidades VMware ofrece mitigaciones alternativas disponibles en el siguiente enlace.

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2024-22252.
- CVE-2024-22253.
- CVE-2024-22254.
- CVE-2024-22255.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY