Vulnerabilidades de severidad alta en VMware

CYBERZAINTZA-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

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 **2 vulnerabilidades** de **severidad alta,** con los identificadores CVE-2024-22246**,** CVE-2024-22248, y **1 vulnerabilidad de severidad media**, con el identificador CVE-2024-22247, las cuales afectan a los productos **VMware SD-WAN Edge** y **VMware SD-WAN Orchestrator.**

Estas vulnerabilidades podrían permitir una **ejecución remota de código** a través de una inyección de comandos no autenticada; hacer vulnerable el mecanismo de autenticación y protección faltante; o una **redirección abierta de un usuario**, lo que supone una **alta gravedad con impacto en la confidencialidad** de los sistemas 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 SD-WAN Edge.
- VMware SD-WAN Orchestrator.

3. Análisis técnico

Los detalles de las vulnerabilidades de criticidad alta son los siguientes:

CVE-2024-22246: vulnerabilidad de criticidad alta de inyección de comandos no autenticada que podría permitir a un atacante, con acceso local a la interfaz de usuario del enrutador Edge, obtener el control total del mismo.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **7.4**

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

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

CVE-2024-22248: vulnerabilidad de redirección abierta en el SD-WAN Orchestrator de Vmware, la cual podría permitir a un actor malicioso redirigir a una víctima a un dominio controlado por un atacante debido a un manejo inadecuado de la ruta que conduce a la divulgación de información sensible.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **7.1**

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

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: Requerida
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad:** Baja
- **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 cuanto a la vulnerabilidad CVE-2024-22246, desde VMWare se recomienda:

- VMware SD-WAN (Edge) versiones 5.x, actualizar a la versión 5.0.1+.
- VMware SD-WAN (Edge) versiones 4.x, actualizar a la versión 4.5.1+.

Para la vulnerabilidad CVE-2024-22247, desde VMWare se recomienda:

- VMware SD-WAN (Edge) versiones 4.5.x/5.x, actualizar a KB97391.

Por último, para la vulnerabilidad CVE-2024-22248, desde VMWare se recomienda:

- VMware SD-WAN (Orchestrator) versiones 5.x, actualizar a la versión 5.0.1+.

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2024-22246.
- CVE-2024-22248.
- CVE-2024-22247.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY