Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

ALERTA DE SEGURIDAD EN VMWARE: EXPLOTACIÓN ACTIVA DE VULNERABILIDADES ZERO-DAY

05 / 03 / 2025

CONTENIDO

INTRODUCCIÓN

En un mundo donde la virtualización es fundamental para la operación de empresas modernas, las vulnerabilidades en plataformas clave como VMware pueden tener un impacto devastador. Recientemente, Broadcom, la empresa matriz de VMware, ha emitido una alerta de seguridad (VMSA-2025-0004) sobre tres vulnerabilidades zero-day en explotación activa: CVE-2025-22224, CVE-2025-22225 y CVE-2025-22226. Estas fallas afectan a productos ampliamente utilizados, como VMware ESXi, vSphere, Workstation, Fusion, Cloud Foundation y Telco Cloud Platform, permitiendo a atacantes con privilegios de administrador o root escapar del entorno de una máquina virtual y tomar control del hipervisor.

Dado que estas vulnerabilidades ya están siendo explotadas, es crucial que las organizaciones actúen de inmediato para proteger sus entornos virtualizados. En esta noticia, te explicamos en detalle qué productos están afectados, cómo funcionan estas vulnerabilidades y qué pasos debes seguir para mitigar los riesgos. La seguridad proactiva y la aplicación oportuna de parches son esenciales para evitar consecuencias graves en un panorama de ciberamenazas cada vez más sofisticado.

ALERTA DE SEGURIDAD EN VMWARE: EXPLOTACIÓN ACTIVA DE VULNERABILIDADES ZERO-DAY

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_03_05_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	05/03/2025
Es día cero (0 day):	Sí

RESUMEN

Broadcom, la empresa matriz de VMware, ha emitido una alerta de seguridad (VMSA-2025-0004) sobre tres vulnerabilidades críticas en sus productos.
Estas fallas, actualmente en explotación activa, afectan a soluciones clave como VMware ESXi, vSphere, Workstation, Fusion, Cloud Foundation y Telco Cloud Platform.
Las vulnerabilidades permiten a atacantes con privilegios de administrador o root en una máquina virtual escapar del entorno de la VM y acceder al hipervisor, lo que representa un riesgo grave para las empresas que dependen de infraestructuras virtualizadas.

Detalles de las Vulnerabilidades
Según el comunicado oficial de Broadcom, estas son las vulnerabilidades identificadas:

1. CVE-2025-22224 (Crítica, CVSS 9.3):
    - Tipo: Desbordamiento de heap en VCMI.
    - Impacto: Permite a atacantes locales con privilegios administrativos ejecutar código como el proceso VMX en el host.
2. CVE-2025-22225 (Alta, CVSS 8.2):
    - Tipo: Escritura arbitraria en ESXi.
    - Impacto: Facilita el escape del sandbox al permitir escrituras arbitrarias en el kernel.
3. CVE-2025-22226 **(Media, CVSS 7.1)**:
    - **Tipo**: Divulgación de información en HGFS.
    - **Impacto**: Permite a los atacantes filtrar memoria del proceso VMX.

Estas fallas son especialmente peligrosas para entornos multiinquilino y empresas que utilizan VMware para cargas de trabajo críticas.

¿Quiénes están afectados?
Las vulnerabilidades impactan a los siguientes productos:

- **VMware ESXi**
- **VMware vSphere**
- **VMware Workstation**
- **VMware Fusion**
- **VMware Cloud Foundation**
- **VMware Telco Cloud Platform**

Si su organización utiliza versiones sin parches de estos productos, estás en riesgo. Es importante destacar que productos como **VMware vCenter**, **SDDC Manager**, **NSX** y **Aria Suite** no están afectados.

Además, Broadcom ha aclarado que deshabilitar **VMware Tools** no elimina el riesgo, ya que los atacantes con acceso privilegiado pueden reactivarlo.

¿Cómo se explotan estas vulnerabilidades?
Los atacantes necesitan tener privilegios de administrador o root en una máquina virtual para explotar estas fallas. Una vez dentro, pueden escapar del entorno de la VM y tomar control del hipervisor, lo que les permite acceder a otros sistemas y datos críticos.

Recomendaciones para Proteger tu Organización
Broadcom ha confirmado que no existen soluciones alternativas viables para estas vulnerabilidades. Por lo tanto, es crucial aplicar los parches de inmediato. A continuación una lista de acciones recomendadas:

1. **Aplica los parches**: Instala las actualizaciones de seguridad más recientes siguiendo las instrucciones del comunicado oficial.
2. **Evalúa el riesgo**: Identifica si tus sistemas están expuestos y prioriza la aplicación de parches en los más críticos.
3. **Monitorea actividad sospechosa**: Revisa logs y actividad del sistema en busca de indicadores de compromiso.
4. **Refuerza controles de acceso**: Limita el acceso administrativo y utiliza autenticación robusta, como MFA (autenticación multifactor).
5. **Implementa segmentación de red**: Restringe el movimiento lateral en entornos virtualizados para minimizar el impacto de un posible ataque.

Conclusión
Las vulnerabilidades en VMware representan un riesgo crítico para las empresas que dependen de infraestructuras virtualizadas. La explotación activa de estas fallas subraya la importancia de actuar rápidamente. Asegúrate de aplicar los parches recomendados y fortalecer las medidas de seguridad para proteger tus sistemas y datos.

La seguridad proactiva es clave en un panorama de ciberamenazas en constante evolución.

NOTICIA COMPLETA

https://devel.group/blog/alerta-de-seguridad-en-vmware-explotacion-activa-de-vulnerabilidades-zero-day/

CONTACTOS DE SOPORTE

Correo electrónico: soporte@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group