	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°250	Fecha: 20-10-2023
		Página: 6 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en productos VMWare		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

VMware ha reportado múltiples vulnerabilidades de severidad **ALTA** de tipo lectura fuera de límites, TOCTOU (Time-of-check Time-of-use) y escalada de privilegios local en Workstation y Fusion. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante obtener información confidencial y elevar privilegios en un sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-34044 de tipo lectura fuera de límites que existe en la funcionalidad para compartir dispositivos Bluetooth host con la máquina virtual en VMware Workstation y Fusion. Un atacante con privilegios administrativos locales en una máquina virtual puede leer información privilegiada contenida en la memoria del hipervisor desde una máquina virtual.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-34045 de tipo de escalada de privilegios local que ocurre durante la instalación por primera vez (el usuario necesita arrastrar o copiar la aplicación a una carpeta desde el volumen '.dmg') o al instalar una actualización. Un atacante con privilegios de usuario local no administrativo puede aprovechar esta vulnerabilidad para escalar privilegios a root en el sistema donde Fusion está instalado o donde se instala por primera vez.

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2023-34046 de tipo TOCTOU (Time-of-check Time-of-use), que ocurre durante la instalación por primera vez (el usuario necesita arrastrar o copiar la aplicación a una carpeta desde el volumen '.dmg') o al instalar una actualización en VMware Fusion. Un atacante con privilegios de usuario local no administrativo puede aprovechar esta vulnerabilidad para escalar privilegios a root en el sistema donde Fusion está instalado o donde se instala por primera vez.

A. Productos afectados:

- VMware Workstation Pro / Reproduction (Workstation), version 17.x y anterior a 17.5.
- VMware Fusion, versión 13.x y anterior a 13.5.

3. RECOMENDACIÓN:

- Actualizar los productos afectados con la última versión de software disponible que abordan estas vulnerabilidades.

Fuente de Información:	• hxxps://www.vmware.com/security/advisories/VMSA-2023-0022.html • hxxps://docs.vmware.com/en/VMware-Fusion/13.5/rn/vmware-fusion-135-release-notes/index.html • hxxps://docs.vmware.com/en/VMware-Workstation-Player/17.5/rn/vmware-workstation-175-player-release-notes/index.html • hxxps://docs.vmware.com/en/VMware-Workstation-Pro/17.5/rn/vmware-workstation-175-pro-release-notes/index.html