DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 099**	**Fecha: 27-04-2023**
		Página 18 de 22

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

Descripción

1. **Resumen:**

VMware ha reportado múltiples vulnerabilidades de severidad **CRÍTICA** de tipo desbordamiento de búfer basada en la pila, escalada de privilegios (stack) y lectura/escritura fuera de límites en varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario, elevar privilegios y acceder a información privilegiada.

2. **Detalles:**

- La vulnerabilidad registrada con el código CVE-2023-20869 de severidad **crítica,** de tipo desbordamiento de búfer basada en la pila (stack) que existe en la funcionalidad para compartir dispositivos Bluetooth host con la máquina virtual. 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 que se ejecuta en el host.

- La vulnerabilidad registrada con el código CVE-2023-20870 de severidad **alta,** de tipo lectura fuera de los límites que existe en la funcionalidad para compartir dispositivos host Bluetooth con la máquina virtual. Un actor malicioso con privilegios administrativos locales en una máquina virtual puede leer información privilegiada contenida en la memoria del hipervisor desde una máquina virtual.

- La vulnerabilidad registrada con el código CVE-2023-20871 de severidad **alta,** de tipo escalada de privilegios. Un actor malicioso con acceso de lectura/escritura al sistema operativo del host puede elevar los privilegios para obtener acceso de root al sistema operativo del host.

- La vulnerabilidad registrada con el código CVE-2023-20872 de severidad **alta,** de tipo lectura /escritura fuera de límites en la emulación de dispositivos de CD/DVD SCSI. Un atacante malintencionado con acceso a una máquina virtual que tiene una unidad de CD/DVD física conectada y configurada para usar un controlador SCSI virtual puede aprovechar esta vulnerabilidad para ejecutar código en el hipervisor desde una máquina virtual.

3. **Productos afectados:**

- Workstation, versiones 17.x ejecutándose en cualquier sistema operativo;
- Fusion, versiones 13.X ejecutándose en OS X.

4. **Solución:**

- Se recomienda instalar los productos afectados con las últimas versiones de software disponibles desde el sitio web del proveedor que corrigen estas vulnerabilidades:
  - Workstation: 17.0.2;
  - Fusion: 13.0.2.

Fuentes de información	▪ hxxps://www.vmware.com/security/advisories/VMSA-2023-0008.html