

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°056		Fecha: 05-03-2024
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en VMware Workstation y Fusion		
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			
<p>1. ANTECEDENTES:</p> <p>Se ha reportado una vulnerabilidad de severidad ALTA de tipo uso después de la liberación y divulgación de información en VMware Workstation y Fusion. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto la ejecución de código en la máquina donde está instalado Workstation o Fusion y obtener acceso a información confidencial.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad alta identificada por MITRE como CVE-2024-22252 de tipo uso después de la liberación, existe debido a un error de uso después de la liberación en el controlador USB XHCI. Un atacante remoto con acceso administrativo al sistema operativo invitado puede desencadenar un error de uso después de la liberación y ejecutar código arbitrario en el sistema operativo host.</p> <p>La vulnerabilidad de severidad alta identificada por MITRE como CVE-2024-22253 de tipo uso después de la liberación, existe debido a un error de uso después de la liberación en el controlador USB UHCI. Un atacante remoto con acceso administrativo al sistema operativo invitado puede desencadenar un error de uso después de la liberación y ejecutar código arbitrario en el sistema operativo host.</p> <p>La vulnerabilidad de severidad media identificada por MITRE como CVE-2024-22255 de tipo divulgación de información, existe debido a una salida excesiva de datos en el controlador USB UHCI. Un usuario remoto con acceso administrativo al sistema operativo invitado puede leer la memoria del proceso vmx.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> – VMware Fusion: 13.0 - 13.5. – VMware Workstation: 17.0 - 17.5. <p>3. RECOMENDACIÓN:</p> <ul style="list-style-type: none"> • Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades. 			
Fuente de Información:	<ul style="list-style-type: none"> • https://www.vmware.com/security/advisories/VMSA-2024-0006.html 		