CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Bad VIB(E)s en hipervisor ESXi

Fecha: **29/09/2022**

Problemática: **Persistencia de malware novedoso dentro de los hipervisor ESXi**

Correlativo: **AA-0026**

Institución / Sector: **Instituciones Públicas y Privadas**

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	**Preventiva**

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	**Alta**	**Alta**	**Alta**

CONTEXTO

Se ha identificado la persistencia de malware novedoso dentro de los hipervisores ESXi, esta amenaza afecta a productos de VMware ESXi, servidores Linux vCenter y máquinas virtuales de Windows. Hasta el momento no se tiene evidencia de que el atacante haya utilizado una vulnerabilidad de día cero para obtener acceso inicial para implementar los "VIB" maliciosos.

SITUACIÓN

De acuerdo al análisis realizado por el Centro Estratégico de Monitoreo - CEM, La técnica utilizada por el atacante no había sido documentada anteriormente; debido a que este aprovechó los paquetes de instalación maliciosos de vSphere ("VIB") para instalar varias puertas traseras en los hipervisores ESXi, las puertas traseras fueron denominadas cómo VIRTUALPITA y VIRTUALPIE. Los VIB maliciosos observados se etiquetaron como PartnerSupported, los archivos de firma estaban vacíos por lo que el atacante modificó el archivo descriptor XML para cambiar el acceptance-levelcampo de communitya partner. Un CommunitySupportednivel de aceptación indica que el VIB fue creado por un tercero que no fue revisado ni firmado por VMware o sus socios de confianza. Esto indicaba que el atacante enmascaró estos archivos VIB como PartnerSupportedsi solo cumplieran con los requisitos de un CommunitySupported VIB. Esto también indicó que el VIB fue creado por una persona o empresa fuera de los programas de socios de VMware y no pasó por ningún programa de aprobado por VMware.

El ataque proveniente de un proceso legítimo de VMware Tools vmtoolsd.exe, en una máquina virtual de Windows alojada en un hipervisor VMware ESXi.
La explotación exitosa permite a un actor de amenazas realizar las siguientes acciones:

- **Mantener un acceso administrativo persistente al hipervisor.**
- **Enviar comandos al hipervisor que se enrutarán a la máquina virtual invitada para su ejecución.**
- **Transferir archivos entre el hipervisor ESXi y las máquinas invitadas que se ejecutan debajo de él.**
- **Manipular los servicios de registro en el hipervisor.**
- **Ejecutar comandos arbitrarios desde una VM invitada a otra VM invitada que se ejecuta en el mismo hipervisor.**

RECOMENDACIONES

Se recomienda a las organizaciones que utilizan ESXi y el conjunto de infraestructura de VMware que sigan los pasos de refuerzo descritos en este link https://www.mandiant.com/resources/blog/esxi-hypervisors-detection-hardening para minimizar la superficie del ataque de los hosts ESXi.

VMware ha desarrollado una guía de mitigación y detección específicamente para las técnicas descritas en el informe de Mandiant Guía de mitigación y búsqueda de amenazas para paquetes de instalación de vSphere sin firmar (VIB) en ESXi (89619) https://kb.vmware.com/s/article/89619

Proteger vSphere del malware especializado https://core.vmware.com/vsphere-esxi-mandiant-malware-persistence

Además de implementar varias prácticas recomendadas de seguridad operativa mencionadas en Proteger vSphere de malware especializado para evitar un posible compromiso en primer lugar, VMware recomienda habilitar la función Secureboot en ESXi para mitigar el riesgo de que los actores maliciosos persistan en un host ESXi comprometido a través de instalación maliciosa de VIB. El arranque seguro se diseñó para no permitir la instalación de VIB sin firmar en un host ESXi. Además, el arranque seguro no permite el indicador --force que normalmente permitiría a un administrador omitir la configuración del nivel de aceptación en el host ESXi.

REFERENCIAS

Investigación realizada por MANDIANT
https://www.mandiant.com/resources/blog/esxi-hypervisors-malware-persistence

Proteger vSphere del malware especializado https://core.vmware.com/vsphere-esxi-mandiant-malware-persistence

Detección y endurecimiento dentro de los hipervisores ESXi
https://www.mandiant.com/resources/blog/esxi-hypervisors-detection-hardening

DICCIONARIO DE DATOS

1. **Ciberdelincuente: Persona que se aprovecha de fallas de seguridad encontradas en plataformas, programas o sistemas a título personal**
2. **Código Arbitrario (RCE): Hace referencia, en el campo de la seguridad informática, a la capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad.**
3. **Hipervisores: Capa entre una máquina puramente virtual y el sistema físico en el que se encuentra una máquina (computadora, servidor)**
4. **Zero Day: Son aquellas vulnerabilidades en sistemas o programas informáticos que son únicamente conocidas por determinados atacantes y son desconocidas por los fabricantes y usuarios. Al ser**

ÁREA PARA DEFINICIONES