Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

DESCUBIERTA VULNERABILIDAD EN ESXI HYPERVISOR EXPLOTADA POR OPERADORES DE RANSOMWARE

29 / 07 / 2024

CONTENIDO

INTRODUCCIÓN

Microsoft ha descubierto una vulnerabilidad crítica en los hipervisores ESXi que está siendo explotada por operadores de ransomware. Esta vulnerabilidad, catalogada como CVE-2024-37085, permite a los atacantes obtener permisos administrativos completos en los hypervisores ESXi unidos a un dominio, facilitando la encriptación masiva de sistemas y el potencial robo de datos.

DESCUBIERTA VULNERABILIDAD EN ESXI HYPERVISOR EXPLOTADA POR OPERADORES DE RANSOMWARE

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

ID de alerta:	DSOC-CERT_2024_01_31_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	29/07/2024
Es día cero (0 day):	No

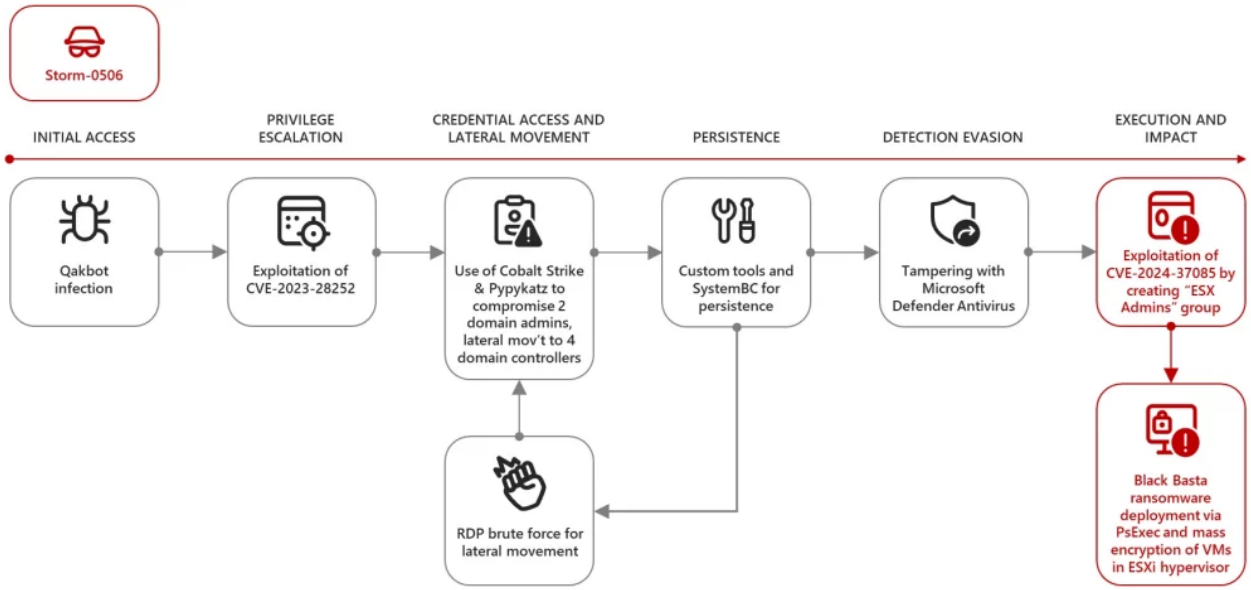
RESUMEN

Vulnerabilidad y Explotación

Microsoft ha identificado una grave vulnerabilidad en los hypervisores ESXi, ampliamente utilizados para gestionar máquinas virtuales en servidores físicos. La vulnerabilidad CVE-2024-37085 permite a los atacantes crear o modificar un grupo de dominio llamado “ESX Admins” que, por defecto, obtiene acceso administrativo completo sin validación adecuada. Esta falla permite a los atacantes encriptar el sistema de archivos del hypervisor, afectando la funcionalidad de los servidores alojados y potencialmente permitiendo el movimiento lateral y la exfiltración de datos.

Grupos de Ransomware Involucrados

Varios grupos de ransomware, incluidos Storm-0506, Storm-1175, Octo Tempest y Manatee Tempest, han sido observados utilizando esta técnica en múltiples ataques. Estos ataques han llevado al despliegue de ransomware como Akira y Black Basta, causando significativas interrupciones en las operaciones de las organizaciones afectadas.



Microsoft ha identificado tres métodos principales para explotar esta vulnerabilidad:

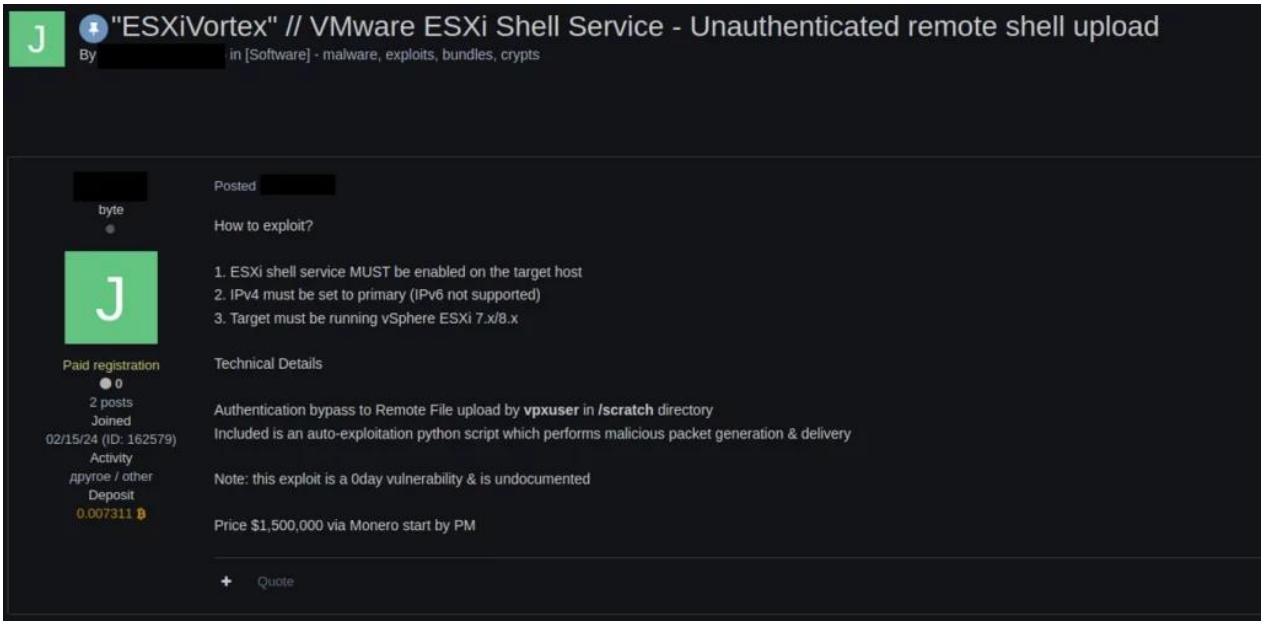
1. Creación del grupo “ESX Admins” y adición de un usuario al grupo: Este método ha sido observado activamente en la naturaleza.

2. Renombrar un grupo existente a “ESX Admins”: Aunque este método no ha sido observado en la naturaleza, es una técnica viable.

3. Refrescar privilegios del hypervisor ESXi: Permite que el grupo “ESX Admins” mantenga privilegios administrativos incluso si se cambian configuraciones.

Incidente Destacado

Un ejemplo destacado de explotación de esta vulnerabilidad ocurrió en una firma de ingeniería en Norteamérica, afectada por un despliegue de ransomware Black Basta por el grupo Storm-0506. Los atacantes obtuvieron acceso inicial mediante una infección de Qakbot, seguida de la explotación de una vulnerabilidad de Windows (CVE-2023-28252), y finalmente, utilizando la vulnerabilidad CVE-2024-37085 para escalar privilegios y encriptar el sistema de archivos ESXi.



Recomendaciones de Seguridad

Microsoft insta a los administradores de servidores ESXi a aplicar inmediatamente las actualizaciones de seguridad proporcionadas por VMware para mitigar esta vulnerabilidad. Además, se recomiendan las siguientes medidas de protección:

- Instalación de Actualizaciones de Software: Asegurarse de instalar las últimas actualizaciones de seguridad en todos los hypervisores ESXi unidos a un dominio.
- Higiene de Credenciales: Proteger cuentas altamente privilegiadas mediante la implementación de autenticación multifactor (MFA) y el uso de métodos de autenticación sin contraseña.
- Mejora de la Postura de Activos Críticos: Identificar y proteger activos críticos en la red con actualizaciones de seguridad, procedimientos de monitoreo adecuados y planes de respaldo y recuperación.
- Detección de Actividades Sospechosas: Configurar detecciones personalizadas en sistemas XDR/SIEM para el nuevo nombre de grupo y monitorear accesos administrativos completos sospechosos.

Conclusión

La vulnerabilidad CVE-2024-37085 representa una amenaza significativa para las organizaciones que utilizan hypervisores ESXi. La colaboración entre investigadores, proveedores y la comunidad de seguridad es crucial para mejorar continuamente las defensas y proteger el ecosistema digital. Microsoft continuará

compartiendo inteligencia y trabajando con la comunidad de seguridad para ayudar a proteger a los usuarios y organizaciones.

NOTICIA COMPLETA

https://devel.group/blog/descubierta-vulnerabilidad-en-esxi-hypervisor-explotada-por-operadores-de-ransomware/

CONTACTOS DE SOPORTE

Correo electrónico: cert@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://www.devel.group/reporta-un-incidente