BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-20
Fecha de publicación: 29/07/2024
Tema: Vulnerabilidad de bypass de autenticacion en VMWare ESXi explotada activamente
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- VMware ESXi 8.0 y 7.0
- VMware Cloud Foundation 5.x y 4.x

Descripción

Esta falla de seguridad de “Omisión de autenticación de integración de Active Directory con VMware ESXi” de gravedad media con un puntaje de 5.8 e identificada como CVE-2024-37085, fue descubierta investigadores de seguridad de Microsoft y solucionada con el lanzamiento de ESXi 8.0 U3 el 25 de junio.

ESXi es un hipervisor de hardware que se instala directamente en un servidor físico y proporciona acceso directo y control de los recursos subyacentes. Los hipervisores ESXi alojan máquinas virtuales que pueden incluir servidores críticos en una red. La vulnerabilidad afecta a un grupo de dominio cuyos miembros tienen acceso administrativo completo al hipervisor ESXi de forma predeterminada, sin la validación adecuada. Aunque un ataque exitoso requiere altos privilegios en el dispositivo de destino y la interacción del usuario.

Microsoft ha informado que varias bandas de ransomware lo están explotando para escalar a privilegios de administrador completos en hipervisores unidos al dominio. Hasta el momento, la vulnerabilidad ha sido explotada por operadores de ransomware identificados como Storm-0506, Storm-1175, Octo Tempest y Manatee Tempest en ataques que han llevado a implementaciones de ransomware Akira y Black Basta.

Microsoft ha identificado al menos tres tácticas que podrían utilizarse para explotar la vulnerabilidad CVE-2024-37085, entre ellas:

- Agregar el grupo "Administradores de ESX" al dominio y agregar un usuario.
- Renombrar cualquier grupo del dominio como "Administradores de ESX" y agregar un usuario al grupo o usar un miembro existente del grupo.
- Actualizar los privilegios del hipervisor ESXi (asignar privilegios de administrador a otros grupos no los eliminará del grupo "Administradores de ESX").

Mitigación

De acuerdo con el fabricante, varias configuraciones avanzadas de ESXi tienen valores predeterminados que no son seguros de manera predeterminada. Al grupo de AD "ESX Admins"se le asigna automáticamente el rol de administrador de VIM cuando un host ESXi se une a un dominio de Active Directory.

Para solucionar el problema, cambie las siguientes opciones avanzadas de ESXi:

- Config.HostAgent.plugins.hostsvc.esxAdminsGroupAutoAdd Desde true a false
- Config.HostAgent.plugins.vimsvc.authValidateInterval Desde 1440 hasta 90
- Config.HostAgent.plugins.hostsvc.esxAdminsGroupde "ESX Admins" a "" (vació)

Obs: esta mitigación ya es abordada en la actualización ESXi 8.0 U3

Solución

- Actualizaciones de VMware: El problema fue solicionado con el parche de seguridad ESXi 8.0 U3. publicadas por VMware para todos los hipervisores ESXi unidos al dominio. Pueden encontrar información al respecto en el siguiente enlace
    - https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505
    - Para ESXi 8.0 https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-esxi-803-release-notes/index.html
    - VMware Cloud Foundation 5.x https://docs.vmware.com/en/VMware-Cloud-Foundation/5.2/rn/vmware-cloud-foundation-52-release-notes/index.html
    - Para ESXi 7.0 y VMware Cloud Foundation 4.x aún no existen parches disponibles.
- Protección de Cuentas Elevadas: Asegúrese de proteger las cuentas con privilegios elevados, especialmente las que pueden administrar otros grupos de dominio.
    - Implemente la autenticación multifactor (MFA) en todas las cuentas y elimine usuarios excluidos de MFA.
    - Habilite métodos de autenticación sin contraseña (e.g., Windows Hello, claves FIDO, Microsoft Authenticator).
    - Use aplicaciones de autenticación para MFA en cuentas que aún requieren contraseñas.
    - Aísle las cuentas privilegiadas de las cuentas de productividad para proteger el acceso administrativo.

Información adicional:

- https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/
- https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-esxi-803-release-notes/index.html
- https://www.bleepingcomputer.com/news/microsoft/microsoft-ransomware-gangs-exploit-vmware-esxi-auth-bypass-in-attacks/
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com