Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CISA recomienda ejecutar acciones sobre vulnerabilidades en VMWare

19/mayo/2022

Contenido

INTRODUCCIÓN

Mediante este boletín, le brindamos toda la información brindada por CISA para aplicar acciones sobre vulnerabilidades presentes en VMWare y poder evitar ataques exitosos a sus plataformas de virtualización de entornos.

VULNERABILIDADES EN VMWARE

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

ID de alerta:	DSOC-CERT_2022_05_19
Clasificación de alerta:	Vulnerabilidad
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**WHITE**
Fecha de publicación:	05/19/2022
Es día cero (0 day):	NO

RESUMEN

Los actores de amenazas, incluidos los probables actores de amenazas persistentes avanzadas (APT), están explotando vulnerabilidades (CVE 2022-22954 y CVE 2022-22960) en los siguientes productos de VMware: VMware Workspace ONE Access (Access), VMware Identity Manager (vIDM), VMware vRealize Automatización (vRA), VMware Cloud Foundation y vRealize Suite Lifecycle Manager. VMware lanzó una actualización para abordar estas vulnerabilidades el 6 de abril de 2022, y los actores de amenazas pudieron aplicar ingeniería inversa a la actualización y comenzar a explotar los productos de VMware afectados que permanecieron sin parches dentro de las 48 horas posteriores al lanzamiento de la actualización.

El 18 de mayo de 2022, VMware lanzó una actualización para dos nuevas vulnerabilidades (CVE-2022-22972 y CVE-2022-22973). Con base en lo anterior, CISA espera que los actores de amenazas desarrollen rápidamente una capacidad para explotar estas vulnerabilidades recientemente lanzadas en los mismos productos de VMware afectados. La explotación de las vulnerabilidades anteriores permite a los atacantes activar una inyección de plantilla del lado del servidor que puede resultar en la ejecución remota de código (CVE-2022-22954); escalar privilegios a 'raíz' (CVE-2022-22960 y CVE-2022-22973); y obtener acceso administrativo sin necesidad de autenticarse (CVE-2022-22972).

CISA ha determinado que estas vulnerabilidades representan un riesgo inaceptable para las agencias del Poder Ejecutivo Civil Federal (FCEB) y requieren una acción de emergencia. Esta determinación se basa en la explotación confirmada de CVE-2022-22954 y CVE-2022-22960 por actores de amenazas en la naturaleza, la probabilidad de explotación futura de CVE-2022-22972 y CVE-2022-22973, la prevalencia de los afectados software en la empresa federal, y el alto potencial de compromiso de los sistemas de información de la agencia.

Tenga en cuenta que los requisitos de las Directivas operativas vinculantes 22-01 y 19-02 de CISA siguen vigentes. CVE 2022-22954 y CVE 2022-22960 se agregaron al catálogo de CISA de vulnerabilidades explotadas conocidas (KEV) el 14 y el 15 de abril de 2022, respectivamente. CISA continuará monitoreando la explotación y agregará KEV al catálogo BOD 22-01 a medida que alcancen los umbrales definidos aquí:
https://www.cisa.gov/known-exploited-vulnerabilities .

CISA recomienda:

1. Enumere todas las instancias de los productos VMware afectados [VMware Workspace ONE Access (Access), VMware Identity Manager (vIDM), VMware vRealize Automation (vRA), VMware Cloud Foundation y vRealize Suite Lifecycle Manager] en las redes de la agencia.

2. Para todas las instancias de productos VMware afectados enumerados en la acción requerida anterior:

A. Implemente actualizaciones según el aviso de seguridad de VMware VMSA-2022-0014 disponible aquí https://www.vmware.com/security/advisories/VMSA-2022-0014.html.

O

B. Eliminar de la red de la agencia hasta que se pueda aplicar la actualización.

Cuando las actualizaciones no estén disponibles debido a que los productos no son compatibles con el proveedor (p. ej., fin del servicio, fin de la vida útil), los productos no compatibles deben eliminarse inmediatamente de las redes de la agencia.

3. Además, para todas las instancias de productos VMware afectados a los que se puede acceder desde Internet:

A. Asumir compromiso, desconectarse inmediatamente de la red de producción y realizar actividades de búsqueda de amenazas como se describe en CISA CSA disponible aquí: www.cisa.gov/uscert/ncas/alerts/aa22-138b

Las agencias pueden volver a conectar estos productos a sus redes solo después de que se completen las actividades de búsqueda de amenazas, no se detecten anomalías y se apliquen las actualizaciones.

RECOMENDACIONES

Se recomiendan las siguientes acciones:

1. Instalar las actualizaciones proporcionadas por VMWare lo mas pronto posible.
2. Si usted posee una versión obsoleta de VMWare, considere migrar a una versión mas reciente que posea soporte del fabricante.
3. Asegúrese que sus servidores cuenten con la protección adecuada de su Firewall, IPS e IDS.
4. Brinde a su SOC los host name o direcciones IP que usted considere de mayor importancia para que puedan ser monitoreadas de manera activa 24/7.

Noticia Completa

https://www.cisa.gov/emergency-directive-22-03

https://therecord.media/cisa-issues-directive-for-exploited-vmware-bug-after-ir-team-deployed-to-large-org/

Enlace de descarga para las actualizaciones.

https://www.vmware.com/security/advisories/VMSA-2022-0014.html

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