Nro. Alerta:	AL-2024-029	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		V 1.1
Fecha:	14-nov-2024	**Vulnerabilidades CVE-2024-38812 y CVE-2024-38813 de VMware vCenter Server**	Pág.: **1** of **5**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de Vulnerabilidad: Ejecución remota de código

Nivel de riesgo: Alto

II. ALERTA

VMware ha lanzado actualizaciones de seguridad para las vulnerabilidades críticas con código CVE-2024-38812 y CVE-2024-38813, con las que un actor malicioso podría realizar la ejecución remota de código en las soluciones de Fundación VMware Cloud y VMware vCenter Server que no se corrigió correctamente en el primer parche de septiembre de 2024.

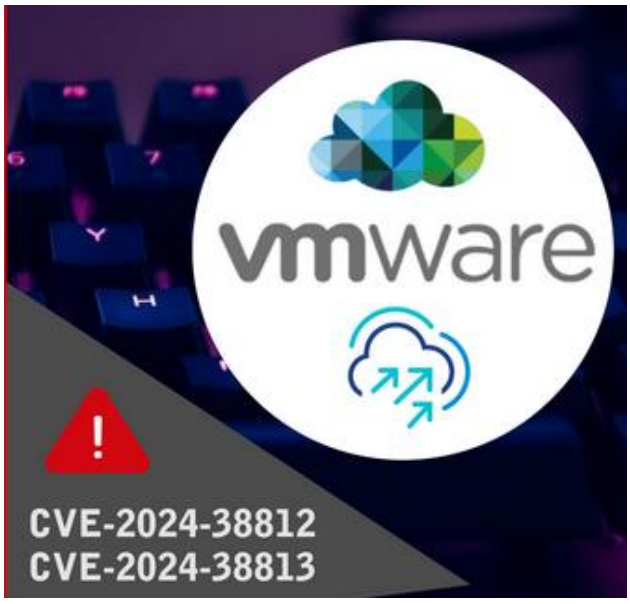

Figura 1: Imagen referencial vulnerabilidades ***CVE-2023-38812 y CVE-2023-38813***

III. INTRODUCCIÓN

VMware, propiedad de la empresa Broadcom, lanzó el pasado 21 de octubre, parches de seguridad para cubrir las vulnerabilidades criticas CVE-2024-38812 y CVE-2024-38813 identificadas en sus plataformas vCenter Server versiones 7.0 y 8.0 y Fundación VMware Cloud versiones 4.x y 5.x.; descubiertas por los equipos de investigación que participaron en la Matrix Cup 2024, un importante concurso de piratería informática en China desarrollado en junio de 2024, donde se identifica vulnerabilidades de día cero en las principales plataformas de sistemas operativos, teléfonos inteligentes, software empresarial, navegadores y productos de seguridad.

La vulnerabilidad crítica CVE-2024-38812 tiene una puntuación de gravedad CVSS de 9,8/10, está documentado como un desbordamiento de pila en la implementación del protocolo DCERPC (Distributed Computing Environment/Remote Procedure Call) dentro de vCenter Server.

VMware advirtió que un atacante con acceso a la red del servidor podría enviar un paquete especialmente diseñado para ejecutar código remoto.

La vulnerabilidad crítica CVE-2024-38813, se describe como una vulnerabilidad de escalada de privilegios con una puntuación de gravedad CVSS máxima de 7,5/10. Un actor malintencionado con acceso de red a vCenter Server puede activar esta vulnerabilidad para escalar privilegios a root mediante el envío de un paquete de red especialmente diseñado.

Broadcom indicó que no tiene conocimiento de ninguna explotación maliciosa de las dos vulnerabilidades expuestas, pero ha instado a los clientes a actualizar las plataformas a las últimas versiones liberadas por el fabricante.

IV. VECTOR DE ATAQUE:

La vulnerabilidad CVE-2024-38812 en VMware vCenter Server afecta a las operaciones que emplean el protocolo DCERPC (Distributed Computing Environment/Remote Procedure Call), utilizado para comunicaciones remotas entre diferentes componentes.

El problema se origina en la forma en que vCenter Server procesa ciertos paquetes de DCERPC, específicamente aquellos que contienen mensajes anómalos o mal formados. Estos mensajes pueden provocar un desbordamiento de memoria en el sistema (heap overflow) al escribir datos más allá de los límites asignados, lo cual puede derivar en la ejecución de código arbitrario con privilegios elevados.

La función `rpc_ss_ndr_unmar_interp` en el contexto de DCERPC en VMware vCenter es una operación de deserialización que maneja la entrada de datos recibida a través de una llamada remota. En la vulnerabilidad CVE-2024-38812, esta función se convierte en un punto débil que podría permitir a un atacante provocar un desbordamiento de búfer en el sistema afectado.

Un atacante puede diseñar un paquete DCERPC que invoque una operación opX_ssr con los parámetros adecuados para que estos sean procesados por rpc_ss_ndr_unmar_interp(), desencadenando el desbordamiento de búfer. La clave de la explotación es seleccionar la operación opX_ssr que tenga el conteo de parámetros y tipos de datos precisos que interactúan de manera insegura con la función de deserialización. Con esta combinación, el atacante puede manipular los datos de entrada para lograr el acceso a memoria fuera de los límites asignados

La explotación depende de la capacidad de manipular punteros de memoria mediante elementos como range_list->lower, que pueden hacer que la aritmética de punteros introduzca direcciones de memoria en regiones no deseadas, lo que lleva a escrituras de memoria arbitrarias. Además, en funciones como rpc_ss_ndr_unmar_by_copying(), las variables controladas por el atacante como copy_length permiten al atacante controlar tanto el destino como la cantidad de datos que se copian, lo que aumenta el riesgo de corrupción de la memoria.

El parche de VMware introduce comprobaciones adicionales en los cálculos de límites de memoria, lo que evita la aritmética de punteros sin límites y reduce el potencial de explotación remota.

V. IMPACTO:

A continuación las versiones vulnerables publicadas en el aviso de seguridad critico de VMWare Nro. VMSA-2024-0019:

Producto VMware	Versión	CVE	Versión CVSS 3	Gravedad	Versión estable
Servidor VMware vCenter	8.0	CVE-2024-38812, CVE-2024-38813	9.8 , 7.5	Crítico	8.0 U3d [1]
Servidor VMware vCenter	8.0	CVE-2024-38812, CVE-2024-38813	9.8 , 7.5	Crítico	8.0 U2e
Servidor VMware vCenter	7.0	CVE-2024-38812, CVE-2024-38813	9.8 , 7.5	Crítico	7.0 U3t [1]
Fundación VMware Cloud	5.x	CVE-2024-38812, CVE-2024-38813	9.8 , 7.5	Crítico	Parche asíncrono para 8.0 U3d [1]
Fundación VMware Cloud	5.1.x	CVE-2024-38812, CVE-2024-38813	9.8 , 7.5	Crítico	Parche asíncrono para 8.0 U2e
Fundación VMware Cloud	4.x	CVE-2024-38812, CVE-2024-38813	9.8 , 7.5	Crítico	Parche asíncrono para 7.0 U3t [1]

Para las versiones anteriores de productos que ya han superado su fecha de fin de soporte, como vSphere 6.5 y 6.7, se verán afectadas, pero no recibirán actualizaciones de seguridad.

VI. RECOMENDACIONES:

- Broadcom advierte que no existe una solución práctica para estos errores. Por lo que, la solución es aplicar los parches de seguridad liberados por el fabricante accesibles a través de los mecanismos de actualización estándar de vCenter Server.

- Los administradores que no puedan aplicar inmediatamente las actualizaciones de seguridad deben controlar estrictamente el acceso del perímetro de la red a los componentes e interfaces de administración de vSphere, incluidos los componentes de almacenamiento y red.

VII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/vmware-fixes-bad-patch-for-critical-vcenter-server-rce-flaw/
- https://www.securityweek.com/vmware-struggles-to-fix-flaw-exploited-at-chinese-hacking-contest/
- https://www.bleepingcomputer.com/news/security/broadcom-fixes-critical-rce-bug-in-vmware-vcenter-server/
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968
- https://www.securityweek.com/vmware-patches-remote-code-execution-flaw-found-in-chinese-hacking-contest/
- https://www.theregister.com/2024/09/17/vmware_vcenter_patch/