Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

VULNERABILIDAD CRÍTICAS DE VCENTER SERVER

25/10/2023

CONTENIDO

INTRODUCCIÓN

VMware ha lanzado actualizaciones de seguridad para solucionar un fallo crítico en vCenter Server que podría provocar la ejecución remota de código en los sistemas afectados.

VULNERABILIDADES CRÍTICAS DE VCENTER SERVER

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

ID de alerta:	DSOC-CERT_2023_10_25_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	25/10/2023
Es día cero (0 day):	No

RESUMEN

VMware ha lanzado actualizaciones de seguridad para solucionar un fallo crítico en vCenter Server que podría provocar la ejecución remota de código en los sistemas afectados.

La compañía dijo que la vulnerabilidad, etiquetada como **CVE-2023-34048**, permite a un actor malintencionado con acceso a la red lanzar exploits de ejecución remota de código, se ha descrito como una vulnerabilidad de escritura fuera de los límites en la implementación del protocolo DCE/RPC.

VMware dijo que no hay soluciones para mitigar la deficiencia y que las actualizaciones de seguridad están disponibles en las siguientes versiones del software:

- VMware vCenter Server 8.0 (8.0U1d u 8.0U2)
- VMware vCenter Server 7.0 (7.0U3o)
- VMware Cloud Foundation 5.x y 4.x

Debido a la naturaleza crítica de este problema, VMware también lanzó parches para productos más antiguos al final de su vida útil, incluidos vCenter Server 6.7U3, 6.5U3, VCF 3.x y vCenter Server 8.0U1. También están disponibles los parches asíncronos de vCenter Server para VCF 5.x y 4.x.

La última actualización aborda además **CVE-2023-34056** (puntuación CVSS: 4,3), una vulnerabilidad de divulgación parcial de información que afecta a vCenter Server y que podría permitir que un actor malintencionado con privilegios no administrativos acceda a datos no autorizados.

VMware, en una sección separada de preguntas frecuentes, dijo que no está al tanto de la explotación de las fallas, pero ha recomendado a los clientes que actúen rápidamente para aplicar los parches lo antes posible para mitigar cualquier amenaza potencial.

MATRIZ DE RESPUESTA

Producto	Versión	Corriendo en	CVE	CVSSv3	Severidad	Solución	Solución Alternativa	Documentación
VMware vCenter Server	8	Cualquiera	CVE-2023-34048, CVE-2023-34056	9.8, 4.3	Crítico	8.0U2	Ninguna	FAQ
VMware vCenter Server	8	Cualquiera	CVE-2023-34048	9.8	Crítico	8.0U1d	Ninguna	FAQ
VMware vCenter Server	7	Cualquiera	CVE-2023-34048, CVE-2023-34056	9.8, 4.3	Crítico	7.0U3o	Ninguna	FAQ
VMware Cloud Foundation (VMware vCenter Server)	5.x, 4.x	Cualquiera	CVE-2023-34048, CVE-2023-34056	9.8, 4.3	Crítico	KB88287	Ninguna	FAQ

RECOMENDACIONES

Para corregir **CVE-2023-34056**, y **CVE-2023-34048**, aplique las actualizaciones enumeradas en la columna "Solución" de la "Matriz de respuesta" ya que no existen soluciones adicionales para corregir esta vulnerabilidad.

NOTICIA COMPLETA

https://devel.group/blog/vulnerabilidad-critica-de-vcenter-server-rce/

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