BEACON LAB

C S I R T

CYBOLT

Security Innovation

Boletín de Alerta

Boletín Nro.: 2023-06
Fecha de publicación: 27/10/2023
Tema: Vulnerabilidades Criticas Reportadas en Productos VMware
Traffic Light Protocol (TLP): White

Productos afectados:

- VMware vCenter Server 8.0 (8.0U1d ó 8.0U2)
- VMware vCenter Server 7.0 (7.0U3o)
- VMware Cloud Foundation 5.x y 4.x
- Aria Operations for Logs version 8.12, 8.10.2, 8.10, 8.8.x, 8.6.x y versions 5.x y 4.x

Descripción:

Se ha reportado una vulnerabilidad critica que afecta a productos VMware vCenter Server que podría resultar en la ejecución remota de código (RCE) en los sistemas afectados.

El problema, identificado como CVE-2023-34048 con puntuación **9.8**, se ha descrito como una vulnerabilidad de escritura fuera de límites en la implementación del protocolo DCE/RPC . "Un actor malicioso con acceso a la red de vCenter Server puede desencadenar una escritura fuera de límites que podría conducir a la ejecución remota de código", dijo VMware en un aviso publicado.

Además, vCenter Server contiene una vulnerabilidad de divulgación parcial de información. VMware ha evaluado la gravedad de este problema en el rango de gravedad moderada identificado como CVE-2023-34056 con una puntuación de **4.3**.

También se ha reportado varias vulnerabilidades en VMware Aria Operations for Logs. Afortunadamente también ya existen actualizaciones disponibles para remediar esta vulnerabilidad.

VMware Aria Operations for Logs contiene dos vulnerabilidad: CVE-2023-34051 de omisión de autenticación y CVE-2023-34052 de mala deserialización. Además, VMware ha evaluado la gravedad de ambas en el rango de gravedad importante con una puntuación de **8.1** cada una.

A la fecha, hemos detectado más de 2.700 servidores vulnerables expuestos, de los cuales hay más de 30 localizados físicamente en Mexico.

Impacto

Un actor malicioso con acceso a la red de vCenter Server puede realizar un ataque out-of-bounds (una escritura fuera de límites) que podría conducir a la ejecución remota de código RCE.

Prevención

El Equipo de VMware han lanzado parches de seguridad para mitigar ambas vulnerabilidades en todos los productos afectados:

- Servidor VMware vCenter 8.0
  - 8.0U2
  - 8.0U1d (solo mitiga CVE-2023-34048)
- Servidor VMware vCenter 7.0
  - 7.0U3o
- VMware Cloud Foundation (servidor VMware vCenter) 5.x, 4.x
  - KB88287
- VMware Aria Operations for Logs
  - Actualizar a version 8.14
  - Para las versions 5.x y 4.x puede utilizar el parche KB95212

Se recomienda planear una actualización de sus productos afectados lo mas pronto possible.

Información adicional:

- https://www.vmware.com/security/advisories/VMSA-2023-0023.html
- https://thehackernews.com/2023/10/act-now-vmware-releases-patch-for.html
- https://www.securityweek.com/vmware-vcenter-flaw-so-critical-patches-released-for-end-of-life-products/
- https://www.vmware.com/security/advisories/VMSA-2023-0021.html

CYBOLT
Security Innovation

BEACON LAB

C S I R T

contact@cybolt.com

cybolt.com