# BOLETÍN DE ALERTA

**Boletín Nro.**: 2024-05
**Fecha de publicación**: 22/01/2024
**Tema**: Vulnerabilidades en VMware vCenter Server y VMware Cloud Foundation

**Productos afectados:**

- VMware vCenter Server versiones 7.0, 8.0
- VMware Cloud Foundation versiones 4.x y 5.x

**Descripción:**

Se han reportado vulnerabilidades para VMWARE vCenter Server, una del tipo ejecución remota de código (*RCE*), identificada como CVE-2023-34048 con una puntuación CVSS de 9.8 (Severidad crítica), y otra, CVE-2023-34056 de divulgación parcial de información con puntuación CVSS de 4.3 (severidad moderada).
Según el fabricante del producto la vulnerabilidad CVE-2023-34048 se produce cuando se registra, un comportamiento de escritura fuera de límites en la implementación del protocolo DCERPC en el sistema afectado. Un actor malicioso con acceso a la red de vCenter Server podría explotar esta vulnerabilidad mediante el envío de consultas especialmente diseñadas al protocolo DCERPC, lo que podría conducir a la ejecución remota de código en el sistema afectado.
El fabricante VMWARE ha reportado que la vulnerabilidad CVE-2023-34048 se encuentra siendo explotada activamente.

**Impacto:**

Un actor malicioso con acceso a la red del vCenter Server puede desencadenar una escritura out-of-bounds (fuera de límites) que potencialmente podría llevar a la ejecución remota de código (CVE-2023-34048).
Un actor malicioso sin privilegios administrativos en vCenter SERVER podría aprovechar esta vulnerabilidad para acceder a datos no autorizados (CVE-2023-34056).

**Recomendación:**

Se recomienda a los administradores aplicar las actualizaciones de la última versión de la página oficial de VMware, también deben realizar un estricto control de acceso perimetral de red a todos los componentes de gestión e interfaces en vSphere y componentes relacionados, como los de almacenamiento y red.

**Información adicional:**

- https://www.bleepingcomputer.com/news/security/vmware-confirms-critical-vcenter-flaw-now-exploited-in-attacks/
- https://www.vmware.com/security/advisories/VMSA-2023-0023.html

- https://nvd.nist.gov/vuln/detail/CVE-2023-34048
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-34056