# BOLETÍN DE ALERTA

**Boletín Nro.**: 2021-24

**Fecha de publicación**: 23/09/2021

**Tema**: Múltiples vulnerabilidades en productos de VMware

.

**Productos afectados:**

- VMware vCenter Server (vCenter Server) versiones 6.5, 6.7 y 7.0.
- VMware Cloud Foundation (Cloud Foundation) versiones 3.x y 4.x.

**Descripción:**

VMware ha corregido 19 vulnerabilidades que afectan a VMware vCenter Server y VMware Cloud Foundation, de las cuales la más crítica es CVE-2021-22005.

**Estas vulnerabilidades tienen los siguientes identificadores:**

- CVE-2021-22005 (Vulnerabilidad de carga de archivos de vCenter Server): de severidad crítica con una puntuación 9.8. VCenter Server contiene una vulnerabilidad de carga de archivos arbitraria en el servicio de análisis. Un actor malintencionado con acceso de red al puerto 443 en vCenter Server puede aprovechar este problema para ejecutar código en vCenter Server cargando un archivo especialmente diseñado. Este problema no afecta a vCenter Server 6.5.

- CVE-2021-21991 (Vulnerabilidad de escalamiento de privilegios locales de vCenter Server): de severidad alta con una puntuación 8.8. VCenter Server contiene una vulnerabilidad de escalamiento de privilegios local debido a la forma en que maneja los tokens de sesión. Un actor malintencionado con acceso de usuario no administrativo en el host de vCenter Server puede aprovechar este problema para escalar privilegios al administrador en vSphere Client (HTML5) o vCenter Server vSphere Web Client (FLEX / Flash).

- CVE-2021-22006 (Vulnerabilidad de omisión del proxy inverso de vCenter Server): de severidad alta con una puntuación 8.3. VCenter Server contiene una vulnerabilidad de omisión de proxy inverso debido a la forma en que los puntos

finales manejan el URI. Un actor malintencionado con acceso de red al puerto 443 en vCenter Server puede aprovechar este problema para acceder a terminales restringidos.

- CVE-2021-22011 (Vulnerabilidad de punto final de API no autenticado del servidor vCenter): de severidad alta con una puntuación 8.1. VCenter Server contiene una vulnerabilidad de punto final de API no autenticado en la biblioteca de contenido de vCenter Server. Un actor malintencionado con acceso de red al puerto 443 en vCenter Server puede aprovechar este problema para realizar una manipulación de la configuración de red de la máquina virtual no autenticada.

- Para el resto de vulnerabilidades de severidad media y baja se han asignado los siguientes identificadores: CVE-2021-22015, CVE-2021-22012, CVE-2021-22013, CVE-2021-22016, CVE-2021-22018, CVE-2021-22014, CVE-2021-22017, CVE-2021-21992, CVE-2021-22007, CVE-2021-22019, CVE-2021-22009, CVE-2021-22010, CVE-2021-22008, CVE-2021-22020 y CVE-2021-21993.

**Impacto:**

La explotación exitosa de las vulnerabilidades puede resultar en un compromiso completo del sistema vulnerable.

**Solución:**

Instalar las actualizaciones del fabricante disponibles en medios oficiales del proveedor.

- Descargas y documentación de vCenter Server 7.0 U2d:
  - https://customerconnect.vmware.com/downloads/details?downloadGroup=VC70U2D&productId=974&rPId=74352
  - https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-vcenter-server-70u2d-release-notes.html
- Descargas y documentación de vCenter Server 6.7 U3o:
  - https://customerconnect.vmware.com/downloads/details?downloadGroup=VC67U3O&productId=742&rPId=73667

- https://docs.vmware.com/en/VMware-vSphere/6.7/rn/vsphere-vcenter-server-67u3o-release-notes.html

- Descargas y documentación de vCenter Server 6.5 U3q:
  - https://customerconnect.vmware.com/downloads/details?downloadGroup=VC65U3Q&productId=614&rPId=74057
  - https://docs.vmware.com/en/VMware-vSphere/6.5/rn/vsphere-vcenter-server-65u3q-release-notes.html
- Descargas y documentación de VMware vCloud Foundation 4.3.1:
  - https://docs.vmware.com/en/VMware-Cloud-Foundation/4.3.1/rn/VMware-Cloud-Foundation-431-Release-Notes.html
- Descargas y documentación de VMware vCloud Foundation 3.10.2.2:
  - https://docs.vmware.com/en/VMware-Cloud-Foundation/3.10.2/rn/VMware-Cloud-Foundation-3102-Release-Notes.html

**Información adicional:**

- https://www.vmware.com/security/advisories/VMSA-2021-0020.html
- https://www.helpnetsecurity.com/2021/09/22/cve-2021-22005/