

BOLETÍN DE ALERTA

Boletín Nro.: 2023-50

Fecha de publicación: 17/11/2023

Tema: Vulnerabilidad Crítica para VMware Cloud Director Appliance

Productos afectados:

- VMware Cloud Director Appliance 10.5.0
- VMware Cloud Director Appliance 10.4.x o inferior

Descripción:

El Fabricante VMware ha publicado un aviso de seguridad relacionado a una vulnerabilidad en el mecanismo de autenticación del producto VMware Cloud Director Appliance, denominada CVE-2023-34060 con severidad asignada de 9.8. Esta vulnerabilidad permitiría a un actor malicioso posicionado en la red interna del dispositivo afectado, obtener acceso a la interfaz de administración aprovechando una vulnerabilidad del tipo *Authentication bypass* evadiendo el control de inicio de sesión en los puertos 22 (ssh) o en el puerto 5480 (consola de gestión del dispositivo). Este bypass no está presente en el puerto 443.

Impacto:

Un actor malicioso podría aprovechar esta vulnerabilidad, para tomar el control total del dispositivo afectado por la vulnerabilidad. Esto permitiría a un actor malicioso acceder a datos confidenciales, realizar cambios en la configuración del dispositivo o incluso interrumpir el servicio.

Solución:

VMWare ha publicado una actualización de software para corregir esta vulnerabilidad. Los usuarios de las versiones afectadas deben aplicar esta actualización lo antes posible para mitigar el riesgo de explotación de esta vulnerabilidad.

Recomendaciones:

Para mitigar el riesgo de explotación de esta vulnerabilidad, VMware recomienda:

- Instalar la actualización de software publicadas en el siguiente [artículo](#)

Información adicional:

- <https://thehackernews.com/2023/11/urgent-vmware-warns-of-unpatched.html>
- <https://www.vmware.com/security/advisories/VMSA-2023-0026.html>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-34060>
- <https://github.com/vmware/photon/wiki/security-advisory-CVE-2023-34060>
- <https://kb.vmware.com/s/article/95534>

Ciberseguridad y Protección de la Información

Ministerio de Tecnologías de la Información y Comunicación (MITIC)

Gral. Santos y Concordia - Complejo Santos - Offic. E14

cert@cert.gov.py | +595 21 217 9000

Asunción - Paraguay | www.cert.gov.py