	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°287	Fecha: 01-12-2023
		Página: 7 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica de omisión de autenticación en dispositivos VMware Cloud Director		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo omisión de autenticación en dispositivos VMware Cloud Director. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto eludir las restricciones de inicio de sesión.

2. DETALLES:

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2023-34060 en los dispositivos VMware Cloud Director (dispositivo VCD), contienen una vulnerabilidad de omisión de autenticación en caso de que el dispositivo VMware Cloud Director se haya actualizado a 10.5 desde una versión anterior.

En una versión actualizada de VMware Cloud Director Appliance 10.5, un actor malintencionado con acceso de red al dispositivo puede eludir las restricciones de inicio de sesión al autenticarse en el puerto 22 (ssh) o el puerto 5480 (consola de administración del dispositivo). Esta omisión no está presente en el puerto 443 (proveedor de VCD e inicio de sesión del inquilino). En una nueva instalación de VMware Cloud Director Appliance 10.5, la omisión no está presente.

El dispositivo VMware Cloud Director se ve afectado porque utiliza una versión de sssd del sistema operativo Photon subyacente. El problema de sssd ya no está presente en las versiones de Photon OS que se envían con sssd-2.8.1-11 o superior (Photon OS 3) o sssd-2.8.2-9 o superior (Photon OS 4 y 5).

Solo las implementaciones que se actualizaron a 10.5 desde una versión anterior se ven afectadas por CVE-2023-34060. Las nuevas implementaciones de 10.5 no se ven afectadas por CVE-2023-34060.

A. Productos afectados:

- Dispositivo VMware Cloud Director, versión 10.5 si se actualiza desde 10.4.x o inferior (Sistema operativo fotón)

3. RECOMENDACIONES:

- Actualizar a VMware Cloud Director Appliance 10.5.1 desde VMware Cloud Director Appliance 10.5.
- Seguir la guía de solución alternativa mencionada en KB95534.

Fuente de Información:	• hxxps://www.vmware.com/security/advisories/VMSA-2023-0026.html • hxxps://github.com/vmware/photon/wiki/security-advisory-CVE-2023-34060