BOLETÍN DE ALERTA

Boletín Nro.: 2021-14

Fecha de publicación: 27/05/2021

Tema: Vulnerabilidades críticas en productos VMware.

Sistemas afectados:

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

Descripción:

VMware ha implementado parches para abordar una vulnerabilidad de seguridad crítica y una de seguridad moderada en el vCenter Server.

La vulnerabilidad crítica está registrada como CVE-2021-21985 (puntuación CVSS 9.8), el problema se debe a la falta de validación de entrada en el complemento de comprobación de estado de Virtual SAN (vSAN), que está habilitado de forma predeterminada en vCenter Server. La versión del parche también rectifica un problema de autenticación en vSphere Client que afecta a Virtual SAN Health Check, Site Recovery, vSphere Lifecycle Manager y VMware Cloud Director Availability plug-ins (CVE-2021-21986, puntaje CVSS: 6.5).

A continuación se expone la lista de vulnerabilidades de gravedad crítica y moderada:

- CVE-2021-21985 es una vulnerabilidad de ejecución remota de código en vSphere Client a través del complemento de verificación de estado de Virtual SAN (vSAN), que está habilitado de forma predeterminada. A esta vulnerabilidad se le asigna una puntuación CVSS de 9.8, lo que la convierte en una falla crítica.

  Para aprovechar esta vulnerabilidad, un atacante debería poder acceder a vCenter Server a través del puerto 443. Incluso si una organización no ha expuesto vCenter Server externamente, los atacantes aún pueden aprovechar esta falla una vez dentro de una red. VMware señala específicamente que los grupos de ransomware son expertos en aprovechar fallas como este compromiso de publicación, después de haber obtenido acceso a una red a través de otros medios. La explotación exitosa

le daría a un atacante la capacidad de ejecutar comandos arbitrarios en el host vCenter subyacente.

- CVE-2021-21986 es un problema del mecanismo de autenticación en varios complementos de vCenter Server, al que se le asigna una puntuación CVSS de 6.5, lo que lo convierte en una gravedad moderada. Puede ser explotada a través del puerto 443 y permitir a un atacante realizar funciones de complemento sin autenticación. Los complementos de vCenter Server afectados incluyen:
  - Comprobación de estado de vSAN
  - Recuperación del sitio
  - Administrador del ciclo de vida de vSphere
  - Disponibilidad de VMware Cloud Director

Impacto:

La explotación exitosa de las vulnerabilidades podría permitir a un atacante remoto ejecutar comandos con privilegios no restringidos en el sistema operativo subyacente que aloja vCenter Server y realizar acciones permitidas por los complementos afectados sin autenticación.

Solución:

- Actualizar los productos afectados a las siguientes versiones:
  - vCenter Server:
    - 7.0 U2b.
    - 6.7 U3n.
    - 6.5 U3p.
  - Cloud Foundation (vCenter Server):
    - 4.2.1.
    - 3.10.2.1.

Información adicional:

- https://www.vmware.com/security/advisories/VMSA-2021-0010.html
- https://es-la.tenable.com/blog/cve-2021-21985-critical-vmware-vcenter-server-remote-code-execution?tns_redirect=true