Alerta de seguridad cibernética	9VSA20-00292-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de agosto de 2020
Última revisión	26 de agosto de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de VMWare referente a dos vulnerabilidades que podrían causar una condición DoS o llevar a un ataque XSS en las aplicaciones afectadas. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-3976
CVE-2020-3975

VMSA-2020-0018

Un atacante con acceso de red a las aplicaciones afectadas podía agotar los recursos en memoria al utilizar los servicios de autenticación, dando como resultado una degradación en el rendimiento de la aplicación durante el ataque y causando una denegación de servicios parcial (Partial DoS).

Productos Afectados

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

Mitigaciones

Para ESXi, aplicar parches ESXi_7.0.0-1.25.16324942, ESXi670-202008101-SG ESXi670-202008401-BG o ESXi650-202007401-BG ESXi650-202007101-SG.
Para Cloud Foundation (ESXi), aplicar parches 4.0.1 o 3.10.0.
Para vCenter Server, aplicar parches 7.0.0b, 6.7u3j o 6.5u3k.
Para Cloud Foundation (vCenter), aplicar parche 4.0.1, el parche para la versión 3.x.x se encuentra pendiente.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2020-0018.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3976

VMSA-2020-0019

Una vulnerabilidad de tipo Cross-site Scripting (XSS) encontrada en App Volumes permitía a un atacante inyectar código malicioso en el explorador de la víctima, ejecutándose al ver el explorador.
Esto era posible debido a que no se validaba correctamente los datos ingresados por el usuario al crear y editar aplicaciones o al crear grupos de almacenamiento, permitiendo la inyección de código.

Productos Afectados

VMWare App Volumes versiones 2.x y 4.

Mitigaciones

Aplicar parche 2.18.6 para la versión 2.x, o parche 2006 para la versión 4.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2020-0019.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3975