Alerta de seguridad cibernética	9VSA20-00230-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de mayo de 2020
Última revisión	02 de mayo 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 múltiples vulnerabilidades que afectan a sus productos. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-3956
CVE-2020-3957
CVE-2020-3958
CVE-2020-3959

CVE-2020-3956

Un atacante remoto y autenticado podría enviar tráfico malicioso hacia la aplicación a través de las interfaces de usuario basadas en HTML5 y en FLEX, la interfaz de explorador de API y acceso a API, la cual podría llevar a la inyección de código arbitrario en el sistema afectado.

Productos Afectados

vCloud Director versiones 10.0.x, 9.7.x y 9.5.x para Linux y PhotonOS y versión 9.1.x para Linux.

Mitigación

Actualizar vCloud Director a la versión 10.0.0.2, 9.7.0.5, 9.5.0.6 o 9.1.0.4, dependiendo de la versión vulnerable que se utilice actualmente.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2020-0010.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3956

CVE-2020-3957

Un atacante local con cuenta de usuario normal podría obtener privilegios de Super Usuario “root” en un sistema donde las aplicaciones afectadas estén instaladas, debido a un error en TOCTOU (Time-of-check Time-of-use) en el abridor de servicio.

Productos Afectados

Fusion versión 11.x para OS X.
VMRC versión 11.x y anteriores para OS X en Mac.
Horizon Client versión 5.x y anteriores para OS X en Mac.

Mitigación

Actualizar Fusion a la versión 11.5.5.
Los parches para VMRC y Horizon Client se encuentran pendientes.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2020-0011.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3957

CVE-2020-3958

Es posible para un atacante causar una denegación de servicios en máquinas virtuales a través de la funcionalidad "shader".
Para una explotación exitosa, se requiere que la máquina tenga las gráficas 3D activadas. Estas vienen por defecto activadas en Workstation y Fusion, pero en ESXi no.

Productos Afectados
ESXi versiones 6.7 y 6.5.
Workstation versión 15.x.
Fusion versión 11.x para OS X.

Mitigación
Para ESXi, aplicar parche ESXi670-202004101-SG o ESXi650-202005401-SG, dependiendo de la versión afectada.
Para Workstation, actualizar a la versión 15.5.2.
Para Fusion, actualizar a la versión 15.5.2.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0011.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3958

CVE-2020-3959

Un atacante local con acceso a una máquina virtual, y sin permisos de administrador, podría causar una denegación de servicios parcial en ella a través de una vulnerabilidad en memoria en el módulo VMCI.

Productos Afectados
ESXi versiones 6.7 y 6.5.
Workstation versión 15.x.
Fusion versión 11.x para OS X.

Mitigación
Para ESXi, aplicar parche ESXi670-202004101-SG o ESXi650-202005401-SG, dependiendo de la versión afectada.
Para Workstation, actualizar a la versión 15.5.2.
Para Fusion, actualizar a la versión 15.5.2.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0011.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3959