

Alerta de seguridad cibernética	9VSA20-00276-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de julio de 2020
Última revisión	18 de julio 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 afectada a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de VMWare respecto a dos vulnerabilidades que afectan a Fusion, VMRC para Mac, Horizon Client para Mac y SD-WAN de VeloCloud. El presente informe incluye las respectivas medidas de mitigación.

Vulnerabilidades

CVE-2020-3973
CVE-2020-3974

CVE-2020-3973

Un atacante malicioso con acceso de inquilino a Velocloud Orchestrator podría enviar sentencias SQL especialmente diseñadas, explotando una vulnerabilidad de validación de datos, y así obtener data que a la cual no debiesen tener acceso.

Productos Afectados

VeloCloud Orchestrador versiones 3.x para Linux.

Mitigaciones

Actualizar a la versión 3.3.2 p2, 3.4.1 y superiores, o aplicar parche a la 3.2.2, 3.3.1, 3.3.2 o 3.4.0 (Contactar servicio técnico de VMWare para obtener el parche).

Enlaces

<https://www.vmware.com/security/advisories/VMSA-2020-0016.html>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3973>

CVE-2020-3974

Debido a que VMware Fusion, VMRC para Mac y Horizon Client para Mac, no validan correctamente el cliente XPC, un atacante con privilegios normales podría explotar esta vulnerabilidad para escalar privilegios y convertirse en usuario root.

Productos Afectados

Fusion versiones 11.x para OS X.

VMRC versiones 11.x y anteriores para OS X.

Horizon Client versiones 5.x y anteriores para OS X.

Mitigaciones

Actualizar a la versión 11.5.5 de Fusion para OS X.

Actualizar a la versión 11.2.0 de VMRC para OS X.

Actualizar a la versión 5.4.3 de Horizon Client para OS X.

Enlaces

<https://www.vmware.com/security/advisories/VMSA-2020-0017.html>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3974>