Alerta de seguridad cibernética	9VSA20-00244-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de junio de 2020
Última revisión	12 de junio 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 afectan a ESXi, Workstation, Fusion y Horizon Client. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-3960
CVE-2020-3961

CVE-2020-3960

Debido a un error de lectura fuera de los límites de la memoria en la funcionalidad NVMe, un atacante local con permisos no administrativos a una máquina virtual podría explotar esta vulnerabilidad para leer información privilegiada en la memoria.

Productos Afectados

VMware vSphere ESXi versiones 6.7 y 6.5.
VMware Workstation Pro/Player versión 15.x.
VMware Fusion Pro/Fusion versión 11.x.

Mitigación

Para VMware vSphere ESXi, actualizar a la versión ESXi670-202006401-SG o ESXi650-202005401-SG.
Para VMware Workstation Pro/Player, actualizar a la versión 15.5.5.
Para VMware Fusion Pro/Fusion, actualizar a la versión 11.5.5.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2020-0012.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3960

CVE-2020-3961

Debido a la insuficiente configuración de permisos de carpetas y a la insegura carga de librerías por parte del software Horizon Client, un atacante local, en donde el software esté instalado, podría aprovecharse de estos fallos para escalar privilegios, logrando la ejecución de código con cualquier usuario del sistema.

Productos Afectados

VMware Horizon Client para Windows versión 5.x y anteriores.

Mitigación

Actualizar a la versión 5.4.3 de VMware Horizon Client para Windows.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2020-0013.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3961