Alerta de seguridad cibernética	9VSA20-00301-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de septiembre de 2020
Última revisión	18 de septiembre 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 seis vulnerabilidades que afectan a Workstation, Fusion y Horizon Client. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-3980
CVE-2020-3986
CVE-2020-3987
CVE-2020-3988
CVE-2020-3989
CVE-2020-3990

CVE-2020-3980

Debido a la forma en que Fusion permite configurar la ruta amplia del sistema, un atacante podría aprovecharse de esto para engañar a un usuario administrador, haciéndole ejecutar código malicioso en el sistema y logrado la elevación de privilegios.

Productos Afectados
VMware Fusion versión 11.x para OS X.

Mitigación
El parche para esta vulnerabilidad se encuentra pendiente.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0020.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3980

CVE-2020-3986, CVE-2020-3987, CVE-2020-3988

Un atacante con acceso normal a una máquina virtual podría causar una denegación de servicios parcial (partial DoS) u obtener información de la memoria desde el proceso TPView, debido a una vulnerabilidad de lectura fuera de los límites en memoria en el componente Cortado ThinPrint.
Esta vulnerabilidad afecta a los parsers EMF, JPEG2000 y STRETCHDIBITS.
Esta vulnerabilidad solo puede explotada si impresión virtual se encuentra activado. Esta característica viene activada por defecto en Horizon Client.

Productos Afectados
VMware Workstation versión 15.x para Windows.
Horizon Client versión 5.x y anteriores para Windows.

Mitigación
Para Workstation, el parche se encuentra pendiente.
Para Horizon Client, actualizar a la versión 5.4.4 para Windows.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0020.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3986
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3987
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3988

CVE-2020-3989

Un atacante con acceso normal a una máquina virtual podría causar una denegación de servicios parcial (partial DoS), debido a una vulnerabilidad de lectura fuera de los límites en memoria en el componente Cortado ThinPrint.
Esta vulnerabilidad solo puede explotada si impresión virtual se encuentra activado. Esta característica viene activada por defecto en Horizon Client.

Productos Afectados
VMware Workstation versión 15.x para Windows.
Horizon Client versión 5.x y anteriores para Windows.

Mitigación
Para Workstation, el parche se encuentra pendiente.
Para Horizon Client, actualizar a la versión 5.4.4 para Windows.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0020.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3989

CVE-2020-3990

Un atacante con acceso normal a una máquina virtual podría causar una denegación de servicios parcial (partial DoS), debido a una vulnerabilidad de lectura fuera de los límites en memoria en el componente Cortado ThinPrint.
Esta vulnerabilidad solo puede explotada si impresión virtual se encuentra activado. Esta característica viene activada por defecto en Horizon Client.

Productos Afectados
VMware Workstation versión 15.x para Windows.
Horizon Client versión 5.x y anteriores para Windows.

Mitigación
Para Workstation, el parche se encuentra pendiente.
Para Horizon Client, actualizar a la versión 5.4.4 para Windows.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0020.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3990