Alerta de seguridad cibernética	9VSA20-00253-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de junio de 2020
Última revisión	26 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 múltiples vulnerabilidades que afectan a sus productos. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-3962
CVE-2020-3963
CVE-2020-3964
CVE-2020-3965
CVE-2020-3966
CVE-2020-3967
CVE-2020-3968
CVE-2020-3969
CVE-2020-3970
CVE-2020-3971

CVE-2020-3962

Debido a un error de uso de memoria luego de ser liberada en el dispositivo SVGA, un atacante local con acceso a la máquina virtual (que tenga las gráficas 3D activadas), podría explotar la vulnerabilidad para realizar la ejecución de código remoto en el hipervisor desde la máquina virtual.
Impacto: crítico.

Productos Afectados

ESXi versión 7.0, 6.7 y 6.5.
Fusion versión 11.x.
Workstation versión 15.x.
Cloud Foundation versión 4.x y 3.x.

Mitigación

Para la versión 7.0 de ESXi, aplicar parche ESXi_7.0.0-1.20.16321839.
Para la versión 6.7 de ESXi, aplicar parche ESXi670-202004101-SG.
Para la versión 6.5 de ESXi, aplicar parche ESXi650-202005401-SG.
Para Fusion, actualizar a la versión 11.5.5.
Para Workstation, actualizar a la versión 15.5.5.
Para la versión 4.0 de Cloud Foundation, el parche 4.0.1 se encuentra pendiente.
Para la versión 3.0 de Cloud Foundation, actualizar a la versión 3.10.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2020-0015.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3962

CVE-2020-3963

Debido a un error de uso de memoria luego de ser liberada en PVNVRAM, un atacante local con acceso a la máquina virtual podría explotar la vulnerabilidad para lograr leer información privilegiada desde la memoria del hipervisor de la máquina virtual.
Impacto: moderado

Productos Afectados

ESXi versión 7.0, 6.7 y 6.5.
Fusion versión 11.x.
Workstation versión 15.x.
Cloud Foundation versión 4.x y 3.x.

Mitigación

Para la versión 7.0 de ESXi, aplicar parche ESXi_7.0.0-1.20.16321839.
Para la versión 6.7 de ESXi, aplicar parche ESXi670-202004101-SG.
Para la versión 6.5 de ESXi, aplicar parche ESXi650-202005401-SG.
Para Fusion, actualizar a la versión 11.5.2.

Para Workstation, actualizar a la versión 15.5.2.
Para la versión 4.0 de Cloud Foundation, el parche 4.0.1 se encuentra pendiente.
Para la versión 3.0 de Cloud Foundation, actualizar a la versión 3.10.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0015.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3963

CVE-2020-3964

Un atacante local con acceso a la máquina virtual podría explotar la vulnerabilidad en el controlador USB EHCI para lograr leer información privilegiada desde la memoria del hipervisor de la máquina virtual.
Impacto: importante

Productos Afectados
ESXi versión 7.0, 6.7 y 6.5.
Fusion versión 11.x.
Workstation versión 15.x.
Cloud Foundation versión 4.x y 3.x.

Mitigación
Para la versión 7.0 de ESXi, aplicar parche ESXi_7.0.0-1.20.16321839.
Para la versión 6.7 de ESXi, aplicar parche ESXi670-202004101-SG.
Para la versión 6.5 de ESXi, aplicar parche ESXi650-202005401-SG.
Para Fusion, actualizar a la versión 11.5.2.
Para Workstation, actualizar a la versión 15.5.2.
Para la versión 4.0 de Cloud Foundation, el parche 4.0.1 se encuentra pendiente.
Para la versión 3.0 de Cloud Foundation, actualizar a la versión 3.10.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0015.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3964

CVE-2020-3965

Un atacante local con acceso a la máquina virtual podría explotar la vulnerabilidad en el controlador USB XHCI para lograr leer información privilegiada desde la memoria del hipervisor de la máquina virtual.
Impacto: importante

Impacto: importante

Productos Afectados
ESXi versión 7.0, 6.7 y 6.5.

Fusion versión 11.x.
Workstation versión 15.x.
Cloud Foundation versión 4.x y 3.x.

Mitigación
Para la versión 7.0 de ESXi, aplicar parche ESXi_7.0.0-1.20.16321839.
Para la versión 6.7 de ESXi, aplicar parche ESXi670-202004101-SG.
Para la versión 6.5 de ESXi, aplicar parche ESXi650-202005401-SG.
Para Fusion, actualizar a la versión 11.5.2.
Para Workstation, actualizar a la versión 15.5.2.
Para la versión 4.0 de Cloud Foundation, el parche 4.0.1 se encuentra pendiente.
Para la versión 3.0 de Cloud Foundation, actualizar a la versión 3.10.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0015.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3965

CVE-2020-3966

Debido a un error desbordamiento en el montículo (HEAP) causado por una condición de carrera en el controlador USB 2.0 EHCI, un atacante local con acceso a la máquina virtual podría explotar la vulnerabilidad para realizar la ejecución de código remoto en el hipervisor desde la máquina virtual.
Impacto: importante

Productos Afectados
ESXi versión 7.0, 6.7 y 6.5.
Fusion versión 11.x.
Workstation versión 15.x.
Cloud Foundation versión 4.x y 3.x.

Mitigación
Para la versión 7.0 de ESXi, aplicar parche ESXi_7.0.0-1.20.16321839.
Para la versión 6.7 de ESXi, aplicar parche ESXi670-202004101-SG.
Para la versión 6.5 de ESXi, aplicar parche ESXi650-202005401-SG.
Para Fusion, actualizar a la versión 11.5.2.
Para Workstation, actualizar a la versión 15.5.2.
Para la versión 4.0 de Cloud Foundation, el parche 4.0.1 se encuentra pendiente.
Para la versión 3.0 de Cloud Foundation, actualizar a la versión 3.10.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0015.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3966

CVE-2020-3967

Debido a un error desbordamiento en el montículo (HEAP) causado por una condición de carrera en el controlador EHCI, un atacante local con acceso a la máquina virtual podría explotar la vulnerabilidad para realizar la ejecución de código remoto en el hipervisor desde la máquina virtual.
Impacto: importante

Productos Afectados

ESXi versión 7.0, 6.7 y 6.5.
Fusion versión 11.x.
Workstation versión 15.x.
Cloud Foundation versión 4.x y 3.x.

Mitigación

Para la versión 7.0 de ESXi, aplicar parche ESXi_7.0.0-1.20.16321839.
Para la versión 6.7 de ESXi, aplicar parche ESXi670-202004101-SG.
Para la versión 6.5 de ESXi, aplicar parche ESXi650-202005401-SG.
Para Fusion, actualizar a la versión 11.5.2.
Para Workstation, actualizar a la versión 15.5.2.
Para la versión 4.0 de Cloud Foundation, el parche 4.0.1 se encuentra pendiente.
Para la versión 3.0 de Cloud Foundation, actualizar a la versión 3.10.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2020-0015.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3967

CVE-2020-3968

Debido a un error de escritura fuera de los limites en memoria en el controlador USB 3.0 xHCI, un atacante local privilegios administrativos en una máquina virtual podría explotar la vulnerabilidad para causar una denegación de servicios o la ejecución de código remoto desde la máquina virtual al hipervisor.
Impacto: importante.

Productos Afectados

ESXi versión 7.0, 6.7 y 6.5.
Fusion versión 11.x.
Workstation versión 15.x.
Cloud Foundation versión 4.x y 3.x.

Mitigación

Para la versión 7.0 de ESXi, aplicar parche ESXi_7.0.0-1.20.16321839.
Para la versión 6.7 de ESXi, aplicar parche ESXi670-202004101-SG.
Para la versión 6.5 de ESXi, aplicar parche ESXi650-202005401-SG.

Para Fusion, actualizar a la versión 11.5.2.
Para Workstation, actualizar a la versión 15.5.2.
Para la versión 4.0 de Cloud Foundation, el parche 4.0.1 se encuentra pendiente.
Para la versión 3.0 de Cloud Foundation, actualizar a la versión 3.10.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0015.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020- CVE-2020-3968

CVE-2020-3969

Debido a un error de desbordamiento del montículo (HEAP) en el dispositivo SVGA, un atacante local con acceso a la máquina virtual (que tenga las gráficas 3D activadas), podría explotar la vulnerabilidad para realizar la ejecución de código remoto en el hipervisor desde la máquina virtual.
Impacto: importante.

Productos Afectados
ESXi versión 7.0.
Fusion versión 11.x.
Workstation versión 15.x.
Cloud Foundation versión 4.x y 3.x.

Mitigación
Para la versión 7.0 de ESXi, aplicar parche ESXi_7.0.0-1.20.16321839.
Para Fusion, actualizar a la versión 11.5.2.
Para Workstation, actualizar a la versión 15.5.2.
Para la versión 4.0 de Cloud Foundation, el parche 4.0.1 se encuentra pendiente.
Para la versión 3.0 de Cloud Foundation, actualizar a la versión 3.10.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0015.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3969

CVE-2020-3970

Debido a un error de lectura fuera de los límites en memoria en la funcionalidad "Shader", un atacante local sin acceso administrativos con acceso a la máquina virtual (que tenga las gráficas 3D activadas), podría explotar la vulnerabilidad para causar una denegación de servicios.
Impacto: importante.

Productos Afectados
ESXi versión 7.0, 6.7 y 6.5.
Fusion versión 11.x.
Workstation versión 15.x.

Cloud Foundation versión 4.x y 3.x.

Mitigación
Para la versión 7.0 de ESXi, aplicar parche ESXi_7.0.0-1.20.16321839.
Para la versión 6.7 de ESXi, aplicar parche ESXi670-202004101-SG.
Para la versión 6.5 de ESXi, aplicar parche ESXi650-202005401-SG.
Para Fusion, actualizar a la versión 11.5.2.
Para Workstation, actualizar a la versión 15.5.2.
Para la versión 4.0 de Cloud Foundation, el parche 4.0.1 se encuentra pendiente.
Para la versión 3.0 de Cloud Foundation, actualizar a la versión 3.10.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0015.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3970

CVE-2020-3971

Debido a un error desbordamiento del montículo (HEAP) en el adaptador virtual de red "vmxnet3", un atacante local sin acceso con acceso a la máquina virtual podría explotar la vulnerabilidad para obtener acceso a información privilegiada en la memoria del hipervisor de la máquina virtual.
Impacto: moderado.

Productos Afectados
ESXi versión 6.7 y 6.5.
Fusion versión 11.x.
Workstation versión 15.x.
Cloud Foundation versión 3.x.

Mitigación
Para la versión 6.7 de ESXi, aplicar parche ESXi670-202004101-SG.
Para la versión 6.5 de ESXi, aplicar parche ESXi650-202005401-SG.
Para Fusion, actualizar a la versión 11.5.2.
Para Workstation, actualizar a la versión 15.5.2.
Para la versión 3.0 de Cloud Foundation, actualizar a la versión 3.10.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0015.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3971