Alerta de seguridad informática	9VSA-00086-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de noviembre de 2019
Última revisión	15 de noviembre de 2019

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 entregada por VMware, referente a vulnerabilidades en sus diferentes productos, las cuales permiten a una atacante local generar ataques de tipo Denegación de Servicios, ejecución de código y obtención de información sin autenticación. También se comparte sus respectivas formas de mitigarlas.

Vulnerabilidades

CVE-2019-5540
CVE-2019-5541
CVE-2019-5542
CVE-2018-12207
CVE-2019-11135
CVE-2018-12126
CVE-2018-12127
CVE-2018-12130
CVE-2019-11091

Impactos

CVE-2018-12207, CVE-2019-11135.
Un atacante con acceso local podría ejecutar código en una máquina virtual, para provocar una pantalla de diagnóstico morada, o un reinicio inmediato del Hypervisor alojado en la máquina virtual, resultando en una condición de denegación de servicios. También puede inferir datos que debiesen estar protegidos por los mecanismos arquitectónicos desde otra máquina virtual o del propio Hypervisor (esta vulnerabilidad solo afecta a los hipervisores que utilizan microarquitectura de procesadores escalables Intel® Xeon® de segunda generación, anteriormente conocidos como Cascade Lake).

Productos Afectados

VMware ESXi 6.7
VMware ESXi 6.5
VMware ESXi 6.0
VMware Workstation 15.x
VMware Fusion 11.x

Mitigación

Para mitigar estas vulnerabilidades, en el caso de ESXi, se deben aplicar todos los parches de las versiones arregladas, y luego seguir las instrucciones en el artículo KB para cada producto en específico. Para el resto de los productos, actualizar a la versión indicada.

Para ESXi 6.7: ESXi 670-201911401-BG, ESXi 670-201911402-BG
https://docs.vmware.com/en/VMware-vSphere/6.7/rn/esxi670-201911001.html

Para ESXi 6.5: ESXi 650-201911401-BG, ESXi 650-201911402-BG
https://docs.vmware.com/en/VMware-vSphere/6.5/rn/esxi650-201911001.html

Para ESXi 6.0: ESXi 600-201911401-BG, ESXi 600-201911402-BG
https://docs.vmware.com/en/VMware-vSphere/6.0/rn/esxi600-201911001.html

Artículo KB: https://kb.vmware.com/s/article/59139

Para VMware Workstation Pro y Player 15.x actualizar a la versión 15.5.1
Para VMware Fusion 11.x actualizar a la versión 15.5.1

Enlaces

https://www.vmware.com/security/advisories/VMSA-2019-0020.html
https://nvd.nist.gov/vuln/detail/CVE-2018-12207
https://nvd.nist.gov/vuln/detail/CVE-2019-11135

Impactos

CVE-2019-5540, CVE-2019-5541, CVE-2019-5542.
El adaptador de red virtual e1000e presenta una vulnerabilidad “out-of-bounds” la cual, al ser explotada, podría llevar a la ejecución de código en el host desde el invitado, o a una denegación de servicios.
Una vulnerabilidad de tipo exposición de información, presente en vmnetdhcp, podría permitir a un atacante acceder a información sensible a través de esta fuga de información en la máquina host.
Existe una vulnerabilidad de tipo denegación de servicios en el controlador RPC la cual podría ser gatillada por un atacante con privilegios de usuario, en su propia VM.

Productos Afectados

VMware Workstation 15.x
VMware Fusion 11.x

Mitigación

Aplicar las actualizaciones correspondientes para cada producto:

Para VMware Workstation Pro y Player 15.x actualizar a la versión 15.5.1
Para VMware Fusion 11.x actualizar a la versión 15.5.1

Enlaces

https://www.vmware.com/security/advisories/VMSA-2019-0021.html
https://nvd.nist.gov/vuln/detail/CVE-2019-5540
https://nvd.nist.gov/vuln/detail/CVE-2019-5541
https://nvd.nist.gov/vuln/detail/CVE-2019-5542

Impactos

CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091.
Un atacante con acceso local a la máquina virtual, y la capacidad de ejecutar código, podría inferir datos que debiesen estar protegidos por los mecanismos arquitectónicos desde otra máquina virtual, del propio Hypervisor odel sistema operativo invitado (Intra-VM), a través de las vulnerabilidades de MDS. Estas vulnerabilidades no afectan a los hipervisores que utilizan

microarquitectura de procesadores escalables Intel® Xeon® de segunda generación, anteriormente conocidos como Cascade Lake.

Productos Afectados

VMware ESXi 6.7
VMware ESXi 6.5
VMware ESXi 6.0
VMware vCenter 6.7
VMware vCenter 6.5
VMware vCenter 6.0
VMware Workstation 15.x
VMware Fusion 11.x
vCloud Usage Meter x.x
Identity Manager x.x
vCenter Server 6.7
vCenter Server 6.5
vCenter Server 6.0
VMware Data Protection 6.x
VMware Integrated Containers 1.x
vRealize Automation 7.x
vRealize Automation 6.x

Mitigación

Para mitigar estas vulnerabilidades, se deben aplicar todos los parches de las versiones arregladas, y luego seguir las instrucciones en el artículo KB para cada producto en específico.

Para vCenter 6.7: actualizar a 6.7 U2a
Para vCenter 6.5: actualizar a 6.5 U2g
Para vCenter 6.0: actualizar a 6.0 U3i
Para ESXi 6.7: ESXi 670-201911401-BG, ESXi 670-201911402-BG
Para ESXi 6.5: ESXi 650-201905401-BG, ESXi 650-201905402-BG
Para ESXi 6.0: ESXi 600-201905401-BG, ESXi 600-201905402-BG
Artículo KB: https://kb.vmware.com/s/article/67577
Artículo KB: https://kb.vmware.com/s/article/68024

Para VMware Workstation Pro y Player 15.x actualizar a la versión 15.5.1
Para VMware Fusion 11.x actualizar a la versión 11.5.0
Artículo KB: https://kb.vmware.com/s/article/68025
Artículo KB: https://kb.vmware.com/s/article/68024

Para vCenter 6.7: actualizar a 6.7u2c

Para vCenter 6.5: actualizar a 6.5u3
Para vCenter 6.0: parche pendiente
vCloud Usage Meter x.x: parche pendiente
Identity Manager x.x: parche pendiente
VMware Data Protection 6.x: parche pendiente
VMware Integrated Containers 1.x: parche pendiente
vRealize Automation 6.x: no tendrá parche
vRealize Automation 7.x: parche pendiente

Enlaces

https://www.vmware.com/security/advisories/VMSA-2019-0008.html
https://nvd.nist.gov/vuln/detail/CVE-2018-12126
https://nvd.nist.gov/vuln/detail/CVE-2018-12127
https://nvd.nist.gov/vuln/detail/CVE-2018-12130
https://nvd.nist.gov/vuln/detail/CVE-2019-11091

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.11.15 08:35:01 -03'00'