Alerta de seguridad informática	9VSA-00052-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de septiembre de 2019
Última revisión	20 de septiembre 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 acerca de 6 vulnerabilidades, 3 de ellas crítica, que afectan a VMWare, sus productos afectados y las mitigaciones correspondientes.

Vulnerabilidades

CVE-2017-16544
CVE-2019-5531
CVE-2019-5532
CVE-2019-5534
CVE-2019-5527
CVE-2019-5535

Producto Afectado

VMware vSphere ESXi (ESXi) versiones 6.7, 6.5 y 6.0.

Impacto

Vulnerabilidad de inyección de comandos en una versión vulnerable de 'busybox' que no sanitiza los nombres de archivos, lo cual puede resultar en una ejecución de cualquier secuencia de escape en Shell.

Mitigaciones

Actualizar a las siguientes versiones de **ESXi**:
Para 6.7 - ESXi670-201904101-SG
Para 6.5 - ESXi650-201907101-SG
Para 6.0 - ESXi600-201909101-SG

Enlaces

https://www.vmware.com/security/advisories/VMSA-2019-0013.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-16544

Productos Afectados

ESXi VMware Host Client versiones 6.7, 6.5 y 6.0.
vCenter Server vSphere Client (HTML5) versiones 6.7 y 6.5.
vCenter Server vSphere Web Client (FLEX/Flash) versions 6.7, 6.5, 6.0.

Impactos

Una vulnerabilidad de divulgación de información en clientes que surge de una caducidad de sesión insuficiente.

Mitigaciones

Actualizar a las siguientes versiones de **ESXi**:
Para 6.7 - ESXi670-201904101-SG
Para 6.5 - ESXi650-201907101-SG
Para 6.0 - ESXi600-201909101-SG

Actualizar a las siguientes versiones de **vCenter**:
Para 6.7 – 6.7 U3
Para 6.5 - 6.5 U3
Para 6.0 - 6.0 U3j

Enlaces

https://www.vmware.com/security/advisories/VMSA-2019-0013.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5531

Producto Afectado

VMware vCenter Server (vCenter) versiones 6.7, 6.5 y 6.0.

Impacto

Una vulnerabilidad de divulgación de información catalogada crítica debido al registro de credenciales en texto plano para máquinas virtuales levantadas a través de OVF.

Mitigaciones

Actualizar a las siguientes versiones de **vCenter**:
Para 6.7 – 6.7 U3
Para 6.5 - 6.5 U3
Para 6.0 - 6.0 U3j

Enlaces

https://www.vmware.com/security/advisories/VMSA-2019-0013.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5532

Producto Afectado

VMware vCenter Server (vCenter) versiones 6.7, 6.5 y 6.0.

Impacto

Máquinas virtuales con OVF podrían exponer información de conexión a través de las propiedades de vAppConfig de la máquina.

Mitigaciones

Actualizar a las siguientes versiones de **vCenter:**
Para 6.7 – 6.7 U3
Para 6.5 - 6.5 U3
Para 6.0 - 6.0 U3j

Enlaces

https://www.vmware.com/security/advisories/VMSA-2019-0013.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5534

Productos Afectados

VMware vSphere ESXi (ESXi) versions 6.7, 6.5, 6.0.
VMware Workstation Pro / Player (Workstation) version 15.x.
VMware Fusion Pro / Fusion (Fusion) version 11.x
VMware Horizon Client para Windows, Linux y Mac versions 5.x y anteriores.
VMRC para Windows y Linux versions 10.x.

Impactos

Vulnerabilidad de acceso a memoria luego de ser liberada en el dispositivo de sonido virtual.
Un atacante local sin acceso de administrador en una máquina huésped podría explotar esta vulnerabilidad para ejecutar código en el host.

Mitigaciones

Actualizar a las versiones de los siguientes productos.

Workstation actualizar a la versión 15.5.0
Fusion actualizar a la versión 11.5.0
VMRC para Windows y Linux actualizar a la versión 10.0.5 y siguientes.
Horizon Client para Windows, Linux y Mac actualizar a la versión 5.2.0.
ESXi 6.7 actualizar a ESXi670-201904101-SG
ESXi 6.5 actualizar a ESXi650-201907101-SG
ESXi 6.0 actualizar a ESXi600-201909101-SG

Enlaces

https://www.vmware.com/security/advisories/VMSA-2019-0014.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5527

Producto Afectado

VMware Workstation Pro / Player (Workstation) version 15.x.
VMware Fusion Pro / Fusion (Fusion) version 11.x

Impactos

Vulnerabilidad DoS (Denegación de Servicios) de red debido al manejo inadecuado de ciertos paquetes IPv6. Un atacante podría enviar paquetes IPV6 especialmente diseñados desde una máquina huésped en VMware NAT para no permitir el acceso de red de todas las máquinas huéspeds que usan el modo VMware NAT.

Mitigaciones

Workstation actualizar a la versión 15.5.0
Fusion actualizar a la versión 11.5.0

Enlaces

https://www.vmware.com/security/advisories/VMSA-2019-0014.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5535

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.09.20 13:37:31 -03'00'