

VMsa-2021-0028.2

10 de Diciembre del 2021

Según un comunicado emitido por el fabricante VMware el día 10 de Diciembre del año 2021, se detectó una vulnerabilidad: **CVE-2021-44228**

¿Cómo me afecta?

CVE-2021-44228

Se detectó un exploit sobre **Apache Log4j** que permite al atacante obtener acceso total al Sistema vulnerado.

¿A quiénes afecta?

Los productos afectados (con sus respectivas versiones) son los siguientes:

Product	Version	Fixed Version	Workarounds
VMware Horizon	8.x, 7.x	Patch Pending	KB87073
VMware vCenter Server	7.x, 6.7.x, 6.5.x	Patch Pending	KB87081
VMware vCenter Server	6.7.x, 6.5.x	Patch Pending	KB87096
VMware HCX	4.2.x, 4.0.x	Patch Pending	KB87104
VMware HCX	4.1.x	Patch Pending	KB87104
VMware NSX-T Data Center	3.x, 2.x	Patch Pending	KB87086
VMware Unified Access Gateway	21.x, 20.x, 3.x	Patch Pending	KB87092
VMware Workspace ONE Access	21.x, 20.10.x	Patch Pending	KB87090
VMware Identity Manager	3.3.x	Patch Pending	KB87093
VMware vRealize Operations	8.x	Patch Pending	KB87076
VMware vRealize Operations Cloud Proxy	Any	Patch Pending	KB87080
VMware vRealize Automation	8.x	Patch Pending	KB87120
VMware vRealize Automation	7.6	Patch Pending	KB87121
VMware vRealize Lifecycle Manager	8.x	Patch Pending	KB87097
VMware Carbon Black Cloud Workload Appliance	1.x	Patch Pending	UeX 109167

VMware Carbon Black EDR Server	7.x, 6.x	Patch Pending	UeX 109168
VMware Site Recovery Manager, vSphere Replication	8.3, 8.4, 8.5	Patch Pending	KB87098
VMware Tanzu GemFire	1.14.x, 1.13.x, 1.10.x	Patch Pending	Article Number 13262
VMware Tanzu Greenplum	6.x	Patch Pending	Article Number 13256
VMware Tanzu Operations Manager	2.x	Patch Pending	Article Number 13264
VMware Tanzu Application Service for VMs	2.x	Patch Pending	Article Number 13265
VMware Tanzu Kubernetes Grid Integrated Edition	1.x	Patch Pending	Article Number 13263
VMware Tanzu Observability by Wavefront Nozzle	3.x, 2.x	Patch Pending	None
Healthwatch for Tanzu Application Service	2.x	Patch Pending	None
Healthwatch for Tanzu Application Service	1.x	Patch Pending	None
Spring Cloud Services for VMware Tanzu	3.x	Patch Pending	None
Spring Cloud Gateway for VMware Tanzu	1.x	Patch Pending	Workaround Pending
Spring Cloud Gateway for Kubernetes	1.x	Patch Pending	Workaround Pending
API Portal for VMware Tanzu	1.x	Patch Pending	Workaround Pending
Single Sign-On for VMware Tanzu Application Service	1.x	Patch Pending	Workaround Pending
App Metrics	2.x	Patch Pending	None
VMware vCenter Cloud Gateway	1.x	Patch Pending	KB87081
VMware vRealize Orchestrator	8.x	Patch Pending	KB87120
VMware vRealize Orchestrator	7.6	Patch Pending	KB87122
VMware Cloud Foundation	4.x, 3.x	Patch Pending	KB87095

VMware Workspace ONE Access Connector (VMware Identity Manager Connector)	21.x, 20.10.x, 19.03.0.1	Patch Pending	KB87091
VMware Horizon DaaS	9.1.x, 9.0.x	Patch Pending	KB87101
VMware Horizon Cloud Connector	1.x, 2.x	Patch Pending	None
VMware NSX Data Center for vSphere	6.x	Patch Pending	KB87099
VMware AppDefense Appliance	2.x	Patch Pending	UeX 109180
VMware Cloud Director Object Storage Extension	2.1.x	Patch Pending	Workaround Pending
VMware Cloud Director Object Storage Extension	2.0.x	Patch Pending	KB87102
VMware Telco Cloud Operations	1.x	Patch Pending	Workaround Pending
VMware vRealize Log Insight	8.2, 8.3, 8.4, 8.6	Patch Pending	KB87089
VMware Tanzu Scheduler	1.x	Patch Pending	Article Number 13280
VMware Smart Assurance NCM	10.1.6	Patch Pending	KB87113
VMware Smart Assurance SAM [Service Assurance Manager]	10.1.2, 10.1.5	Patch Pending	KB87119
VMware Integrated OpenStack	7.x	Patch Pending	KB87118
VMware vRealize Business for Cloud	7.x	Patch Pending	KB87127
VMware vRealize Network Insight	5.3, 6.x	Patch Pending	KB87135

Resolución

Al momento de realizar cualquier Workaround se recomienda tomar todas las medidas necesarias de respaldo, para ello se recomienda contar con un backup y tomar un snapshot sin memoria de los equipos.

Algunos de los Workarounds son:

- [vCenter Server](#)
- [vRealize Operations](#)
- [vRealize Log Insight](#)
- [Horizon](#)
- [Unified Access Gateway](#)
- [Site Recovery Manager, vSphere Replication](#)
- [NSX-V](#)
- [NSX-T](#)
- [VCF](#)
- [Identity Manager](#)
- [Tanzu Kubernetes](#)

vCenter Server:

Tareas previas

Las nuevas versiones de vCenter cuentan con un backup nativo por FTP. Es necesario contar este backup antes de realizar las tareas mencionadas. En caso de no poder realizarlo, como alternativa se podrá realizar un snapshot sin memoria (aunque no es el mejor medio de respaldo).

Para aplicar el workaround para CVE-2021-44228 usando un script automatizado, referir al siguiente link:

[Script de Python para automatizar el workaround de la vulnerabilidad VMSA-2021-0028 en el appliance de vCenter Server Appliance](#) (Recomendado)

Para aplicar manualmente el workaround de CVE-2021-44228 a vCenter Server Appliance 7.x y 6.7, avanzar a la sección correspondiente:

[Presionar aquí para ir al workaround de vCenter Server Appliance 7.0.x](#)

[Presionar aquí para ir al workaround de vCenter Server Appliance 6.7.x](#)

[Presionar aquí para ir al workaround de vCenter Server Appliance 6.5.x](#)

[Presionar aquí para ir al workaround de vCenter Server Appliance 6.0.x](#)

Nota: Para vCenter Cloud Gateway, solo es necesario cumplir con los pasos del Servicio vMON y Servicio Analytics.

Workaround de vCenter Server Appliance 7.0.x

Servicio vMON

1. Realizar un backup del archivo java-wrapper-vmon existente

```
cp -rfp /usr/lib/vmware-vmon/java-wrapper-vmon  
/usr/lib/vmware-vmon/java-wrapper-vmon.bak
```

2. Modificar el archivo java-wrapper-vmon con un editor de texto

```
vi /usr/lib/vmware-vmon/java-wrapper-vmon
```

3. Abajo de todo en el archivo, reemplazar la última línea de código con dos nuevas líneas:

El paso 3 se ejecuta según la versión de vCenter corriendo en su ambiente. El reemplazo notado a continuación SOLO aplica a las siguientes versiones de vCenter: vCenter 7.0 Update 3, 3a, 3b y vCenter 7.0 Update 2, 2a, 2b, 2c, 2d

Última línea, original

```
exec $java_start_bin $jvm_dynargs $security_dynargs $original_args
```

Últimas líneas, luego del cambio

```
log4j_arg="-Dlog4j2.formatMsgNoLookups=true"  
exec $java_start_bin $jvm_dynargs $log4j_arg $security_dynargs  
$original_args
```

El reemplazo notado a continuación SOLO aplica a las siguientes versiones de vCenter:

- vCenter 7.0 GA, 7.0.0a, 7.0.0b, 7.0.0c, 7.0.0d
- vCenter 7.0 Update 1, U1a, U1c, U1d

Última línea, original

```
exec $java_start_bin $jvm_dynargs "$@"
```

Últimas líneas, luego del cambio

```
log4j_arg="-Dlog4j2.formatMsgNoLookups=true"
```

```
exec $java_start_bin $jvm_dynargs $log4j_arg "$@"
```

4. Asegurar que los permisos de los archivos estén asignados correctamente con los siguientes comandos:

```
chown root:cis /usr/lib/vmware-vmon/java-wrapper-vmon
```

```
chmod 754 /usr/lib/vmware-vmon/java-wrapper-vmon
```

5. Reiniciar los servicios de vCenter

```
service-control --stop --all
```

```
service-control --start --all
```

Servicio de Update Manager

1. Realizar un backup del archivo start.ini existente

```
cp -rfp /usr/lib/vmware-updatemgr/bin/jetty/start.ini /usr/lib/vmware-updatemgr/bin/jetty/start.ini.bak
```

2. Modificar el archivo start.ini con un editor de texto

```
vi /usr/lib/vmware-updatemgr/bin/jetty/start.ini
```

3. Agregar la siguiente línea de comando al final del archivo:

```
-Dlog4j2.formatMsgNoLookups=true
```

4. Reiniciar el servicio de Update Manager

```
service-control --restart vmware-updatemgr
```

Servicio de Analytics

1. Realizar un backup del archivo log4j-core-2.8.2.jar

```
cp -rfp /usr/lib/vmware/common-jars/log4j-core-2.8.2.jar  
/usr/lib/vmware/common-jars/log4j-core-2.8.2.jar.bak
```

2. Ejecutar el comando zip para deshabilitar la clase

```
zip -q -d /usr/lib/vmware/common-jars/log4j-core-2.8.2.jar  
org/apache/logging/log4j/core/lookup/JndiLookup.class
```

3. Reiniciar el servicio Analytics

```
service-control --restart vmware-analytics
```

Verificar los cambios

Al haber realizado los pasos anteriores, usar el siguiente procedimiento para verificar que la implementación haya sido exitosa.

1. Verificar que los servicios de vMON hayan iniciado con el nuevo parámetro “-

```
Dlog4j2.formatMsgNoLookups=true”:  
ps auxww | grep formatMsgNoLookups
```

Chequear que los procesos incluyan lo siguiente: `-Dlog4j2.formatMsgNoLookups=true`

2. Verificar que los cambios de Update Manager aparezcan bajo ‘System Properties’ en el output de los siguientes comandos:

```
cd /usr/lib/vmware-updatemgr/bin/jetty/  
java -jar start.jar --list-config  
System Properties:  
-----  
log4j2.formatMsgNoLookups = true  
(/usr/lib/vmware-updatemgr/bin/jetty/start.ini)
```

3. Verificar los cambios en el servicio de Analytics:

```
grep -i jndilookup /usr/lib/vmware/common-jars/log4j-core-2.8.2.jar | wc -l
```

Este comando previo debería devolver 0 líneas, es decir, nada.

Workaround de vCenter Server Appliance 6.7.x

Servicio de vMON

1. Realizar un backup del archivo java-wrapper-vmon existente

```
cp -rfp /usr/lib/vmware-vmon/java-wrapper-vmon /usr/lib/vmware-vmon/java-wrapper-vmon.bak
```

2. Modificar el archivo java-wrapper-vmon con un editor de texto

```
vi /usr/lib/vmware-vmon/java-wrapper-vmon
```

3. Abajo de todo en el archivo, reemplazar la última línea de código con dos nuevas líneas:

Última línea, original

```
exec $java_start_bin $jvm_dynargs "$@"
```

Últimas líneas, luego del cambio

```
log4j_arg="-Dlog4j2.formatMsgNoLookups=true"
```

```
exec $java_start_bin $jvm_dynargs $log4j_arg "$@"
```

3. Reiniciar los servicios de vCenter

```
service-control --stop --all
```

```
service-control --start --all
```

Nota: Si los servicios no inician, verificar los permisos de los archivos con los siguientes comandos:

```
chown root:cis /usr/lib/vmware-vmon/java-wrapper-vmon
```

```
chmod 754 /usr/lib/vmware-vmon/java-wrapper-vmon
```

Servicio de Analytics

NOTA: El workaround listado a continuación es aplicable solo en vCenter Server 6.7 Update 3o y versiones anteriores. vCenter Server 6.7 Update 3p cubre el workaround por defecto, y se puede verificar el mismo con el comando 'ps auxww'.

1. Realizar un backup del archivo log4j-core-2.8.2.jar

```
cp -rfp /usr/lib/vmware/common-jars/log4j-core-2.8.2.jar
```

```
/usr/lib/vmware/common-jars/log4j-core-2.8.2.jar.bak
```

2. Deshabilitar la clase usando el comando zip

```
zip -q -d /usr/lib/vmware/common-jars/log4j-core-2.8.2.jar
```



```
org/apache/logging/log4j/core/lookup/JndiLookup.class
```

3. Reiniciar el servicio de Analytics

```
service-control --restart vmware-analytics
```

Servicio de CM

1. Realizar un backup del archivo log4j-core-2.8.2.jar

```
cp -rfp /usr/lib/vmware-cm/lib/log4j-core.jar
```

```
/usr/lib/vmware-cm/lib/log4j-core.jar.bak
```

2. Deshabilitar la clase usando el comando zip

```
zip -q -d /usr/lib/vmware-cm/lib/log4j-core.jar
```

```
org/apache/logging/log4j/core/lookup/JndiLookup.class
```

3. Reiniciar el servicio de CM

```
service-control --stop vmware-cm
```

```
service-control --start vmware-cm
```

Servicio de Secure Token

1. Realizar un backup y editar el archivo vmware-stds

```
cp /etc/rc.d/init.d/vmware-stds /root/vmware-stds.bak
```

```
vi /etc/rc.d/init.d/vmware-stds
```

2. Encontrar en el código la sección que comienza con `start_service()`. Insertar la línea de código `"-Dlog4j2.formatMsgNoLookups=true \"` cerca de la línea 266, justo antes de la línea `"$DAEMON_CLASS start"` tal como lo vemos en el ejemplo a continuación:

```
start_service()
{
    perform_pre_startup_actions

    local retval

    JAVA_MEM_ARGS=`/usr/sbin/cloudvm-ram-size -J vmware-stds`

    $JSVC_BIN -procname $SERVICE_NAME \
```

```
-home $JAVA_HOME \  
  
-server \  
  
<snip>  
  
-Dauditlog.dir=/var/log/audit/sso-events \  
  
-Dlog4j2.formatMsgNoLookups=true \  
  
$DAEMON_CLASS start
```

3. Reiniciar el servicio vmware-std

```
service-control --stop vmware-std  
  
service-control --start vmware-std
```

Servicio de Identity Management

1. Realizar un backup y editar el archivo vmware-sts-idmd

```
cp /etc/rc.d/init.d/vmware-sts-idmd /root/vmware-sts-idmd.bak  
  
vi /etc/rc.d/init.d/vmware-sts-idmd
```

2. Insertar la línea de código "-Dlog4j2.formatMsgNoLookups=true \" cerca de la línea 177, antes de la línea "\$DEBUG_OPTS \", tal como vemos en el ejemplo a continuación:

```
$JSVC_BIN -procname $SERVICE_NAME \  
  
-wait 120 \  
  
-server \  
  
<snip>  
  
-Dlog4j.configurationFile=file://$PREFIX/share/config/log4j2.xml  
  
\  
  
-Dlog4j2.formatMsgNoLookups=true \  
  
$DEBUG_OPTS \  
  
$DAEMON_CLASS
```

3. Reiniciar el servicio vmware-sts-idmd

```
service-control --stop vmware-sts-idmd
```

```
service-control --start vmware-sts-idmd
```

Verificar los cambios

Al haber realizado los pasos anteriores, usar el siguiente procedimiento para verificar que la implementación haya sido exitosa.

1. Verificar si los servicios controlados por stsd, idmd, y vMON fueron iniciados con el nuevo parametro “-Dlog4j2.formatMsgNoLookups=true”:

```
ps auxww | grep formatMsgNoLookups
```

Chequear que los procesos incluyan lo siguiente: -Dlog4j2.formatMsgNoLookups=true

2. Verificar los cambios del servicio de Analytics:

```
grep -i jndilookup /usr/lib/vmware/common-jars/log4j-core-2.8.2.jar | wc -l
```

Este comando previo debería devolver 0 líneas, es decir, nada.

3. Verificar los cambios del servicio CM:

```
grep -i jndilookup /usr/lib/vmware-cm/lib/log4j-core.jar | wc -l
```

Este comando previo debería devolver 0 líneas, es decir, nada.

Workaround de vCenter Server Appliance 6.5.x

Servicio vMON

1. Realizar un backup del archivo java-wrapper-vmon existente

```
cp -rfp /usr/lib/vmware-vmon/java-wrapper-vmon /usr/lib/vmware-vmon/java-wrapper-vmon.bak
```

2. Modificar el archivo java-wrapper-vmon con un editor de texto

```
vi /usr/lib/vmware-vmon/java-wrapper-vmon
```

3. Abajo de todo en el archivo, reemplazar la última línea de código con dos nuevas líneas:

Última línea, original

```
exec $java_start_bin $jvm_dynargs "$@"
```

Últimas líneas, luego del cambio

```
log4j_arg="-Dlog4j2.formatMsgNoLookups=true"
```

```
exec $java_start_bin $jvm_dynargs $log4j_arg "$@"
```

3. Reiniciar los servicios de vCenter

```
service-control --stop --all
```

```
service-control --start --all
```

Nota: Si los servicios no inician, verificar los permisos de los archivos con los siguientes comandos:

```
chown root:cis /usr/lib/vmware-vmon/java-wrapper-vmon
```

```
chmod 754 /usr/lib/vmware-vmon/java-wrapper-vmon
```

Servicio de CM

1. Realizar un backup del archivo log4j-core.jar

```
cp -rfp /usr/lib/vmware-cm/lib/log4j-core.jar
```

```
/usr/lib/vmware-cm/lib/log4j-core.jar.bak
```

2. Deshabilitar la clase ejecutando el comando zip

```
zip -q -d /usr/lib/vmware-cm/lib/log4j-core.jar
```

```
org/apache/logging/log4j/core/lookup/IndiLookup.class
```

3. Reiniciar el servicio de CM

```
service-control --stop vmware-cm
```

```
service-control --start vmware-cm
```

Servicio de Secure Token

1. Realizar un backup y editar el archivo vmware-std

```
cp /etc/rc.d/init.d/vmware-std /root/vmware-std.bak
```

```
vi /etc/rc.d/init.d/vmware-std
```

2. Encontrar la sección del código que comienza con `start_service()`. Insertar la línea de código `"-Dlog4j2.formatMsgNoLookups=true \"` cerca de la línea 266, justo antes de la línea `"$DAEMON_CLASS start"` tal como vemos en el ejemplo a continuación:

```
start_service()
```

```
{  
  
perform_pre_startup_actions  
  
local retval  
  
$JSVC_BIN -procname $SERVICE_NAME \  
  
-home $JAVA_HOME \  
  
-server \  
  
<snip>  
  
-Dauditlog.dir=/var/log/audit/sso-events \  
  
-Dlog4j2.formatMsgNoLookups=true \  
  
$DAEMON_CLASS start
```

3. Reiniciar el servicio vmware-std

```
service-control --stop vmware-std  
  
service-control --start vmware-std
```

Servicio de Identity Management

1. Realizar un backup y editar el archivo vmware-std-idmd

```
cp /etc/rc.d/init.d/vmware-std-idmd /root/vmware-std-idmd.bak  
  
vi /etc/rc.d/init.d/vmware-std-idmd
```

2. Insertar la línea de código "-Dlog4j2.formatMsgNoLookups=true \" cerca de la línea 177, antes de la línea "\$DEBUG_OPTS \" tal como lo vemos en el ejemplo a continuación:

```
$JSVC_BIN -procname $SERVICE_NAME \  
  
-wait 120 \  
  
-server \  
  
<snip>  
  
-Dlog4j.configurationFile=file://$PREFIX/share/config/log4j2.xml
```

\

```
-Dlog4j2.formatMsgNoLookups=true \
```

```
$DEBUG_OPTS \
```

```
$DAEMON_CLASS
```

3. Reiniciar el servicio vmware-sts-idmd

```
service-control --stop vmware-sts-idmd
```

```
service-control --start vmware-sts-idmd
```

Servicio del PSC Client

1. Realizar un backup y editar el archivo vmware-psc-client

```
cp -rjp /etc/rc.d/init.d/vmware-psc-client /root/vmware-psc-client.bak
```

```
vi /etc/rc.d/init.d/vmware-psc-client
```

2. Insertar la línea de código "-Dlog4j2.formatMsgNoLookups=true \" cerca de la línea 300, justo antes de la línea "\$DAEMON_CLASS start" tal como vemos en el ejemplo a continuación:

```
$JSVC_BIN -procname $SERVICE_NAME \  
  
-home $JAVA_HOME \  
  
-server \  
  
<snip>  
  
-Djava.io.tmpdir="$CATALINA_BASE/temp" \  
  
-Dlog4j2.formatMsgNoLookups=true \  
  
$DAEMON_CLASS start
```

3. Reiniciar el servicio vmware-psc-client

```
service-control --stop vmware-psc-client
```

```
service-control --start vmware-psc-client
```

Verificar los cambios

Al haber realizado los pasos anteriores, usar el siguiente procedimiento para verificar que la implementación haya sido exitosa.

1. Verificar si los archivos controlados por stsd, idmd, psc-client, y vMON fueron iniciados con el nuevo parametro “-Dlog4j2.formatMsgNoLookups=true”:

```
ps auxww | grep formatMsgNoLookups
```

Chequear que los procesos incluyan lo siguiente: -Dlog4j2.formatMsgNoLookups=true

2. Verificar si hubo cambios en el servicio de CM:

```
grep -i jndilookup /usr/lib/vmware-cm/lib/log4j-core.jar | wc -l
```

Este comando previo debería devolver 0 líneas, es decir, nada.

Workaround de vCenter Server Appliance 6.0 U3j

vCenter Server Appliance 6.0 U3j ya no es cubierto por el soporte general de VMware, pero ha sido identificado como vulnerable a CVE-2021-44228 dado al servicio de Performance Charts. Los pasos a seguir para mitigar esta vulnerabilidad son los siguientes:

1. Realizar un backup y editar el archivo ‘/usr/lib/vmware-perfcharts/wrapper/conf/wrapper.conf’ en el appliance y agregar la siguiente línea de código justo debajo de "wrapper.java.additional.13=-Dlog4j.configurationFile=file:/etc/vmware-perfcharts/log4j2.xml" (línea 72):

```
wrapper.java.additional.14=-Dlog4j2.formatMsgNoLookups=true
```

2. Guardar el archivo, parar el servicio de PerfCharts y luego iniciarlo de nuevo con service-control:

```
service-control --stop vmware-perfcharts
```

```
service-control --start vmware-perfcharts
```

Nota: Las versiones entre vCenter Server Appliance 6.0GA y 6.0U3i no son vulnerables.

No obstante, se encontraron archivos vulnerables, los cuales no se utilizan, en las versiones 6.0 U3a, b, c, d, e y f. Incluso al remover los siguientes archivos, el funcionamiento del producto no se vió afectado.

```
/opt/pivotal/pivotal-tc-server-standard/templates/gemfire-p2p/lib/log4j-core-2.1.jar
```

```
/opt/pivotal/pivotal-tc-server-standard/templates/gemfire-p2p/lib/log4j-api-2.1.jar
```

```
/opt/pivotal/pivotal-tc-server-standard/templates/gemfire-cs/lib/log4j-core-2.1.jar
```

/opt/pivotal/pivotal-tc-server-standard/templates/gemfire-cs/lib/log4j-api-2.1.jar

Wetcom S.A.

vRealize Operations

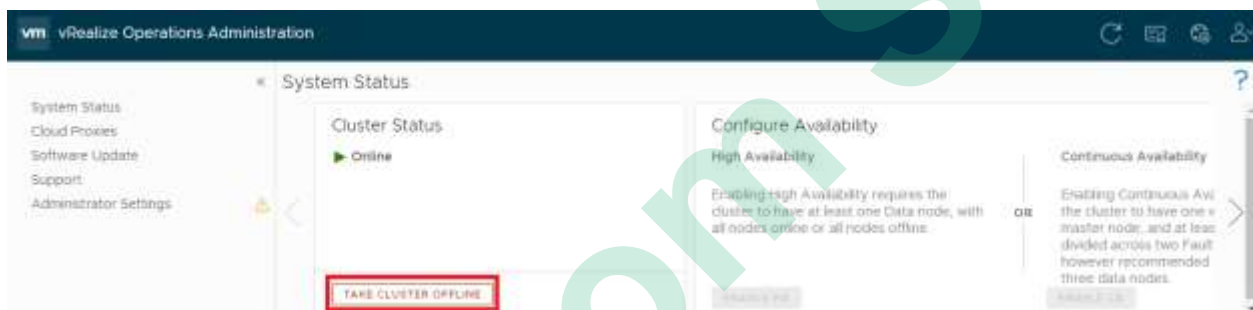
Pasos previos

- Tomar un snapshot de los nodos (sin incluir la memoria de la VM), para asegurar un método de rollback ante cualquier eventualidad.
- Descargar los scripts adjuntos en la siguiente [KB](#)

Procedimiento

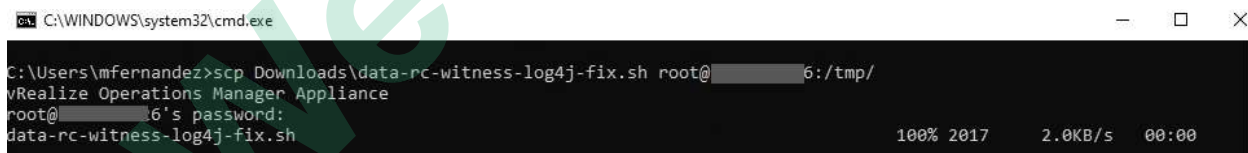
El workaround debe aplicarse para cada nodo (Primario, Réplica, Data), el colector remoto y los nodos Witness.

1. Ingresar a vRealize Operations Manager Admin UI como usuario admin local.
2. Presionar click en **Take Offline** en la sección **Cluster Status**.



Nota: esperar a que el estado del cluster sea **Offline**.

3. Copiar el archivo `data-rc-witness-log4j-fix.sh` al directorio `/tmp` en todos los nodos, por SCP.



4. Ingresar a cada nodo via SSH o por Consola, presionando ALT + F1 en la consola para acceder.
5. Ubicarse en el directorio `/tmp` en todos los nodos:

```
cd /tmp
```

6. Ejecutar el siguiente comando en todos los nodos para que el script `data-rc-witness-log4j-fix.sh` sea ejecutable:

```
chmod +x data-rc-witness-log4j-fix.sh
```

7. Ejecutar el siguiente comando en todos los nodos para ejecutar el script:

```
./data-rc-witness-log4j-fix.sh
```

```
root@ [ /tmp ]# ./data-rc-witness-log4j-fix.sh
*****
Updating file: /usr/lib/vmware-vcops/user/conf/analytics/wrapper.conf
Sucessfully updated file: /usr/lib/vmware-vcops/user/conf/analytics/wrapper.conf
*****
Updating file: /usr/lib/vmware-vcops/user/conf/collector/wrapper.conf
Sucessfully updated file: /usr/lib/vmware-vcops/user/conf/collector/wrapper.conf
*****
Updating file: /usr/lib/vmware-vcops/user/conf/gemfire/wrapper.conf
Sucessfully updated file: /usr/lib/vmware-vcops/user/conf/gemfire/wrapper.conf
*****
Updating file: /usr/lib/vmware-vcops/user/conf/tomcat-enterprise/wrapper.conf
Sucessfully updated file: /usr/lib/vmware-vcops/user/conf/tomcat-enterprise/wrapper.conf
*****
Updating file: /usr/lib/vmware-casa/casa-webapp/bin/setenv.sh
Sucessfully updated file: /usr/lib/vmware-casa/casa-webapp/bin/setenv.sh
*****
Updating file: /usr/lib/vmware-vcops/tomcat-web-app/bin/setenv.sh
Sucessfully updated file: /usr/lib/vmware-vcops/tomcat-web-app/bin/setenv.sh
root@ [ /tmp ]#
```

Nota: asegurarse de que no aparezca ningun mensaje de ERROR como output del script.

8. Ejecutar el siguiente comando en todos los nodos para reiniciar el servicio CaSA

```
service vmware-casa restart
```

9. Ingresar a vRealize Operations Manager Admin UI como usuario admin local.
10. Hacer click en **Bring Online** en **Cluster Status**.



Nota: esperar a que el estado del cluster sea **Online**.

Procedimiento (Cloud Proxy)

En caso de tener nodos Cloud Proxy, el procedimiento es el siguiente:

1. Copiar el archivo `cp-log4j-fix.sh` al directorio `/tmp` en todos los nodos Cloud Proxy.
2. Ingresar a cada nodo Cloud Proxy via SSH o por Consola, presionando ALT + F1 en la consola para acceder.
3. Ubicarse en el directorio `/tmp` en todos los nodos Cloud Proxy

```
cd /tmp
```

4. Ejecutar el siguiente comando en todos los nodos Cloud Proxy para que el script `cp-log4j-fix.sh` sea ejecutable:

```
chmod +x cp-log4j-fix.sh
```

5. Ejecutar el siguiente comando en todos los nodos Cloud Proxy para ejecutar el script:

```
./cp-log4j-fix.sh
```

6. Ejecutar el siguiente comando en todos los nodos Cloud Proxy para reiniciar los servicios Collector y CaSA:

```
service vmware-casa restart  
service collector restart
```

Verificación del workaround

Para corroborar de que el workaround para el **CVE-2021-44228** fue aplicado correctamente en vRealize Operations, se deben seguir los siguientes pasos:

1. Ingresar a cada nodo via SSH o por Consola, presionando Alt + F1 en la consola para ingresar.
2. Ejecutar el siguiente comando para verificar que el workaround fue aplicado exitosamente:

```
ps axf | grep --color log4j2.formatMsgNoLookups | grep -v grep
```

```

root@ [ ~ ]# ps axf | grep --color log4j2.formatMsgNoLookups | grep -v
grep
1017 ?          Sl          4:54 /usr/java/default/bin/java -Djava.util.logging.config
.file=/usr/lib/vmware-casa/casa-webapp/conf/logging.properties -Djava.util.loggi
ng.manager=org.apache.juli.ClassLoaderLogManager -Xmx512M -Xms102M -Xss256K -DAL
IVE_BASE=/usr/lib/vmware-vcops -DSTORAGE_LOG_VCOPS=/storage/log/vcops -Dcasa.aud
it.logfile=/data/vcops/log/casa.audit.log -DVCOPS_DATA_VCOPS=/data/vcops -Djsse.
enableSNIExtension=false -Dnetworkaddress.cache.ttl=60 -XX:MaxJavaStackTraceDept
h=8192 -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/storage/db/vcops/heapdu
mp/ -XX:OnOutOfMemoryError=/usr/lib/vmware-vcops/install/oom-handler.sh %p -Xlog
gc:/storage/log/vcops/log/casa/casa-gc.log -XX:+UseGCLogFileRotation -XX:NumberO
fGCLogFiles=10 -XX:GCLogFileSize=20m -XX:+UseParallelOldGC -XX:NewRatio=2 -XX:Ma
xHeapFreeRatio=60 -XX:MinHeapFreeRatio=40 -XX:+PrintGCDetails -XX:+PrintGCDateSt
amps -XX:+PrintGCApplicationConcurrentTime -XX:+PrintGCApplicationStoppedTime -X
X:+PrintAdaptiveSizePolicy -XX:+PrintHeapAtGC -classpath /usr/java/latest/lib/ex
t/bc-fips-1.0.2.jar:/usr/java/latest/lib/ext/bcpkix-fips-1.0.2.jar:/usr/java/lat
est/lib/ext/bctls-fips-1.0.10.3.jar -Djava.net.preferIPv6Addresses=false -Dorg.b
ouncycastle.fips.approved_only=false -Dlog4j2.formatMsgNoLookups=true -Djdk.tls.
ephemeralDHKeySize=2048 -Djava.protocol.handler.pkgs=org.apache.catalina.webreso
urces -Dorg.apache.catalina.security.SecurityListener.UMASK=0022 -javaagent:/usr
/lib/vmware-vcops/common/lib/vrops-alias-instrumentation-1.0-SNAPSHOT.jar -Dcom.
sun.management.jmxremote -Dcom.sun.management.jmxremote.port=9009 -Dcom.sun.mana
gement.jmxremote.ssl=true -Dcom.sun.management.jmxremote.ssl.config.file=/usr/li
b/vmware-vcops/user/conf/jmxssl.config -Dcom.sun.management.jmxremote.ssl.need.c
lient.auth=false -Dcom.sun.management.jmxremote.registry.ssl=false -Dcom.sun.man
agement.jmxremote.authenticate=true -Dcom.sun.management.jmxremote.access.file=/
usr/lib/vmware-vcops/user/conf/jmxremote.access -Dcom.sun.management.jmxremote.p
assword.file=/usr/lib/vmware-vcops/user/conf/jmxremote.password -Dcom.vmware.vro
ps.jmx.host=localhost -Xbootclasspath/p:/usr/lib/vmware-vcops/./vmware-casa/cas
a-webapp/webapps/casa/WEB-INF/lib/vrops-rmi-1.0-SNAPSHOT.jar -Dignore.endorsed.d
irs= -classpath /usr/share/tomcat/bin/bootstrap.jar:/usr/share/tomcat/bin/tomcat
-juli.jar -Dcatalina.base=/usr/lib/vmware-casa/casa-webapp -Dcatalina.home=/usr/
share/tomcat -Djava.io.tmpdir=/usr/lib/vmware-casa/casa-webapp/temp org.apache.c
atalina.startup.Bootstrap start

```

Nota: debe aparecer un output al ejecutarse el comando. De no aparecer output en cualquiera de los nodos, significa que no se realizó el cambio en esos nodos. Se deberá volver a ejecutar el script en esos nodos, siguiendo los pasos descritos en el procedimiento de ejecución del workaround.

Método de Rollback

Para revertir los cambios realizados por el workaround, se deberá volver al estado anterior de cada nodo utilizando los snapshots tomados previo a la ejecución del workaround.

vRealize Log Insight

REQUISITO PREVIO

- Tomar un snapshot de los nodos (sin incluir la memoria de la VM), para asegurar un método de rollback ante cualquier eventualidad.

Procedimiento

1. Descargar el archivo “**li-log4j-fix.sh**” adjunto en la siguiente [kb](#)
2. Una vez descargado el **archivo “li-log4j-fix.sh”**, copiarlo en el directorio **/tmp** del nodo log insight.
3. Iniciar sesión como **root** en el nodo Log Insight a través de SSH o Consola (ALT+F1).
4. Una vez conectado al nodo, ejecutar los siguientes comandos:

```
cd /tmp  
chmod +x li-log4j-fix.sh  
./li-log4j-fix.sh
```

(Antes de continuar, asegurarse de que no haya mensajes de ERROR en la salida del script)

 - i. Si no hay errores, continuar normalmente
 - ii. Si hay errores, volver a hacer el paso a paso antes de reiniciar.
5. Reiniciar el servicio de vRealize Log Insight con el siguiente comando:

```
service loginsight restart
```
6. En el caso de que exista más de un nodo Log Insight, debe aplicar los pasos descritos anteriormente en cada uno de ellos.

Verificar si el workaround fue aplicado correctamente

Para verificar si el workaround para CVE-2021-44228 fue aplicado correctamente en vRealize Log Insight, debe realizar los siguientes pasos:

1. Iniciar sesión como root a través de SSH o Consola (ALT+F1)
2. Ejecute el siguiente comando para verificar si la solución fue aplicada correctamente:

```
ps axf | grep --color log4j2.formatMsgNoLookups | grep -v grep
```

3. El workaround se habrá aplicado correctamente si luego de ejecutar el comando anterior, hay una salida como la siguiente:

```
root@Insight [ ~ ]# ps axf | grep --color log4j2.formatMsgNoLookups | grep
-v grep
12838 ?          S1l   20:12 /usr/lib/loginsight/application/3rd_party/bin/java -X
rs -Dlog4j2.formatMsgNoLookups=true -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDump
Path=/storage/core/loginsight/var/heapdump/li_heapdump.hprof -XX:ErrorFile=/stor
age/core/loginsight/var/jvm_hs_err_pid.log -Djava.util.logging.config.level=SEVE
RE -Djdk.tls.ephemeralDHKeySize=2048 -Dorg.bouncycastle.fips.approved_only=false
-Djavax.net.ssl.trustStorePassword=changeit -DLOGINSIGHT_HOME=/usr/lib/loginsig
ht -Dstrata.pgid=12818 -cp /usr/lib/loginsight/application/lib/* -Xmx3987m -Xms3
987m -Xss256k -Xmn1024M -XX:+UseConcMarkSweepGC -XX:+UseParNewGC -XX:CMSInitiat
ingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -XX:+ScavengeBeforeFul
lGC -XX:TargetSurvivorRatio=80 -XX:SurvivorRatio=8 -XX:MaxTenuringThreshold=15 -
XX:ParallelGCThreads=4 -XX:+UseCompressedOops -XX:+OptimizeStringConcat -XX:+Alw
aysPreTouch com.vmware.loginsight.daemon.LogInsightDaemon --wait=120
13189 ?          SL1l  16:15 \_ java -Xloggc:/usr/lib/loginsight/application/lib/
apache-cassandra-3.11.9/bin/./logs/gc.log -ea -XX:+UseThreadPriorities -XX:Thre
adPriorityPolicy=42 -XX:+HeapDumpOnOutOfMemoryError -Xss256k -XX:StringTableSize
=1000003 -XX:+AlwaysPreTouch -XX:-UseBiasedLocking -XX:+UseTLAB -XX:+ResizeTLAB
-XX:+UseNUMA -XX:+PerfDisableSharedMem -Djava.net.preferIPv4Stack=true -XX:+UseP
arNewGC -XX:+UseConcMarkSweepGC -XX:+CMSParallelRemarkEnabled -XX:SurvivorRatio=
8 -XX:MaxTenuringThreshold=1 -XX:CMSInitiatingOccupancyFraction=75 -XX:+UseCMSIn
itiatingOccupancyOnly -XX:CMSWaitDuration=10000 -XX:+CMSParallelInitialMarkEnabl
ed -XX:+CMSEdenChunksRecordAlways -XX:+CMSClassUnloadingEnabled -XX:+PrintGCData
ils -XX:+PrintGCDateStamps -XX:+PrintHeapAtGC -XX:+PrintTenuringDistribution -XX
:+PrintGCApplicationStoppedTime -XX:+PrintPromotionFailure -XX:+UseGCLogFileRota
tion -XX:NumberOfGCLogFiles=10 -XX:GCLogFileSize=10M -Dlog4j2.formatMsgNoLookups
=true -Xms1024M -Xmx1024M -Xmn256M -XX:+UseCondCardMark -XX:CompileCommandFile=
/storage/core/loginsight/cidata/cassandra/config/hotspot_compiler -javaagent:/usr
/lib/loginsight/application/lib/apache-cassandra-3.11.9/bin/./lib/jamm-0.3.0.ja
r -Djava.rmi.server.hostname=10.10.6.32 -Dcassandra.jmx.local.port=7199 -Dcom.su
n.management.jmxremote.authenticate=true -Dcom.sun.management.jmxremote.password
.file=/storage/core/loginsight/cidata/cassandra/config/jmxremote.password -Djava
.library.path=/usr/lib/loginsight/application/lib/apache-cassandra-3.11.9/bin/./
/lib/sigar-bin -Dcassandra.consistent.rangemovement=false -XX:OnOutOfMemoryError
=kill -9 %p -Dlogback.configurationFile=logback.xml -Dcassandra.logdir=/usr/lib/
loginsight/application/lib/apache-cassandra-3.11.9/bin/./logs -Dcassandra.stora
gedir=/usr/lib/loginsight/application/lib/apache-cassandra-3.11.9/bin/./data -D
cassandra-foreground=yes -cp /storage/core/loginsight/cidata/cassandra/config:/u
sr/lib/loginsight/application/lib/apache-cassandra-3.11.9/bin/./build/classes/m
ain:/usr/lib/loginsight/application/lib/apache-cassandra-3.11.9/bin/./build/cla
sses/thrift:/usr/lib/loginsight/application/lib/apache-cassandra-3.11.9/bin/./l
ib/airline-0.6.jar:/usr/lib/loginsight/application/lib/apache-cassandra-3.11.9/b
in/./lib/antlr-runtime-3.5.2.jar:/usr/lib/loginsight/application/lib/apache-cas
sandra-3.11.9/bin/./lib/apache-cassandra-3.11.9.jar:/usr/lib/loginsight/applica
tion/lib/apache-cassandra-3.11.9/bin/./lib/apache-cassandra-thrift-3.11.9.jar:/
usr/lib/loginsight/application/lib/apache-cassandra-3.11.9/bin/./lib/asm-5.0.4.
jar:/usr/lib/loginsight/application/lib/apache-cassandra-3.11.9/bin/./lib/caffe
ine-2.2.6.jar:/usr/lib/loginsight/application/lib/apache-cassandra-3.11.9/bin/./
/lib/cassandra-driver-core-3.0.1-shaded.jar:/usr/lib/loginsight/application/lib/
apache-cassandra-3.11.9/bin/./lib/commons-cli-1.1.jar:/usr/lib/loginsight/appli
cation/lib/apache-cassandra-3.11.9/bin/./lib/commons-codec-1.9.jar:/usr/lib/log
insight/application/lib/apache-cassandra-3.11.9/bin/./lib/commons-lang3-3.1.jar
:/usr/lib/loginsight/application/lib/apache-cassandra-3.11.9/bin/./lib/commons-
math3-3.2.jar:/usr/lib/loginsight/application/lib/apache-cassandra-3.11.9/bin/./
/lib/compress-1zf-0.8.4.jar:/usr/lib/loginsight/application/lib/apache-cassandra
-3.11.9/bin/./lib/concurrentlinkedhashmap-lru-1.4.jar:/usr/lib/loginsight/appli
```

En el caso de no tener una salida luego de ejecutar el comando anterior, deberá realizar nuevamente el paso a paso para aplicar el wordkaround para CVE-2021-44228 en vRealize Log Insight.

Horizon

Las soluciones que se describen a continuación funcionarán en las siguientes versiones de VMware Horizon.

Horizon 8 versiones 2111, 2106, 2103, 2012, 2006

Horizon 7 versiones 7.13.1 / 7.13.0 / 7.12.0 / 7.10.3

La siguiente tabla enumera todos los componentes de Horizon e indica las versiones afectadas por CVE-2021-44228 con condiciones vulnerables y soluciones alternativas aplicables. Aparte del componente HTML Access que se enumera a continuación, ningún otro cliente de Horizon se ve afectado.

Horizon Component	Vulnerable Versions	Applicable Workaround
Connection Server	All supported versions (vulnerable only if HTML Access portal is enabled)	Manual or scripted workaround for Horizon Connection Server listed in "Workaround" section.
Windows Agent	2006, 7.13.x, 7.10.x (vulnerable only if vRealize Operations for Horizon desktop agent is enabled/installed)	Workaround pending.
Linux Agent	All supported versions	Manual workaround for Horizon Agent for Linux listed in "Workaround" section.
Linux Agent Direct Connect	All supported versions	Manual workaround for Horizon Agent for Linux listed in "Workaround" section.
HTML Access	All supported versions	Manual or scripted workaround for Horizon Connection Server listed in "Workaround" section.
Cloud Connector	All supported versions	No workaround, must install new 2.1.1 version
vRealize Operations for Horizon Desktop Agent	6.7.1	Workaround pending.
Horizon Recording Server	None[1]	NA
Horizon Recording Agent	None[1]	NA
Universal Broker Plug-in	None[2]	NA[3]
Windows Agent Direct Connect	None[1]	NA
Help Desk	None[2]	NA
GPO Bundle	None[1]	NA
vRealize Operations for Horizon Broker Agent	None[2]	NA
Enrollment Server	None[1]	NA
Security Server	None[2]	NA
JMP Server	None[1]	NA
Persona Agent	None[1]	NA
View Composer	None[1]	NA

Leyenda:

[1] - No vulnerable ya que usa una pila de tecnología que no es Java

[2] - No vulnerable porque el appender log4j2 no está en uso

[3] - Aunque no es vulnerable, se ha publicado una nueva [compilación 21.06](#) ya que los análisis de seguridad mostrarán un , tarro log4j vulnerable.

REQUISITO PREVIO

- Tomar un snapshot de los nodos (sin incluir la memoria de la VM), para asegurar un método de rollback ante cualquier eventualidad.

Procedimiento manual para los Connection Server:

1. Editar el valor de JVMOptions de la siguiente registry key:

```
HKLM\Software\VMware, Inc.\VMware VDM\plugins\wsnm\TomcatService\Params\JVMOptions
```

2. Dejar un espacio al final y agregar el siguiente texto:

```
-Dlog4j2.formatMsgNoLookups=true
```

3. Salir del regedit y reinicie el servicio del servidor de conexión o reinicie el equipo.

Procedimiento por script para los Connection Server:

1. Ejecutar el siguiente script como administrador local

```
@echo off
setlocal
goto start
```

```
CVE-2021-44228 - Prevent log4j parameter expansion
Horizon Connection Server 7.x, 8.x
VMware, Inc. 2021
```

```
:start
set sigpath=HKLM\Software\VMware, Inc.\VMware VDM\plugins\wsnm\TomcatService
for /f "delims=" %%g in ('reg.exe query "%sigpath%" /v Filename') do set sigval=%%g
if "%sigval%"==" " goto notneeded
set killflag=-Dlog4j2.formatMsgNoLookups=true
set svcpath=HKLM\Software\VMware, Inc.\VMware VDM\plugins\wsnm\TomcatService\Params
for /f "tokens=2*" %%v in ('reg.exe query "%svcpath%" /v JVMOptions') do set svcval=%%w
echo %svcval%|find " %killflag%" >nul
if not errorlevel 1 goto notneeded
reg add "%svcpath%" /v JVMOptions /d "%svcval% %killflag%" /f
net stop wsbroker /y && net start wsbroker
echo Completed.
goto :EOF
```

```
:notneeded
echo Not required.
```


goto :EOF

2. Una vez aplicado, el script requerirá un reinicio sobre la máquina.
3. Si esta mitigación ya fue aplicada, no se necesita hacer un reinicio.

Notas:

- *La mitigación se deshará si se reinstala el software, por lo que deberá repetir los procedimientos nuevamente.*
- *Se requiere espacio siguiente para el parámetro.*
- *El parámetro agregado distingue entre mayúsculas y minúsculas.*

Procedimiento manual para agentes Windows:

Se aplica de la misma manera que para el caso de los Connection Server. Tener en cuenta que el agente se encontrará instalado necesariamente sobre la Golden Image y en determinadas VMs en función de los componentes de su infraestructura.

Sea el caso para la Golden Image, es posible que la ubicación de la registry key a modificar sea diferente. Editar el valor del siguiente registro:

```
HKLM\Software\VMware, Inc.\Vmware VDM\Node Manager\JVM
```

El valor que presenta es el siguiente:

```
-Xmx32m -Djdk.tls.ephemeralDHkeySize=2048
```

Y deberá ser modificado de la siguiente manera:

```
-Xmx32m -Djdk.tls.ephemeralDHkeySize=2048 -Dlog4j2.formatMsgNoLookups=true
```

Luego de modificarlo, es necesario reiniciar la vm, luego de iniciar sesión, apagar la misma y tomar un snapshot y actualizar los desktop pools hacia este mismo.

Procedimiento manual para agentes Linux:

1. Según su distribución de Linux, estará presente uno de los siguientes archivos:
 - */usr/lib/vmware/viewagent/bin/StartAgent.sh*
 - */etc/rc.d/init.d/viewagent*
 - */etc/init/viewagent.conf*
 - */etc/init.d/viewagent.suse*
2. Buscar el texto:

`-Dfile.encoding = UTF-8`

3. Modificarlo a:

`-Dlog4j2.formatMsgNoLookups = true -Dfile.encoding = UTF-8`

Nota: No utilice copiar / pegar. Escriba la actualización manualmente

Por ejemplo :

Antes: `exec $ {exec} -Dfile.encoding = UTF-8`

Después: `exec $ {exec} -Dlog4j2.formatMsgNoLookups = true -Dfile.encoding = UTF-8`

4. Guarde y salga del archivo.

5. Reinicie el servicio `viewagent` ejecutando el comando

`sudo service viewagent restart`

Verificación del workaround

Connection Server:

Volviendo a ejecutar el script, debería de indicar el siguiente texto **“Not required.”** Si es que el procedimiento manual o con script han sido ejecutados correctamente

Agente Linux:

Ejecutar el siguiente comando en el agente:

`ps axf | grep --color log4j2.formatMsgNoLookups | grep -v grep`

Si no hay ningún mensaje de respuesta en la consola, el procedimiento no se ha ejecutado correctamente. Para confirmar que se ha ejecutado correctamente debería de tener una respuesta como la siguiente

```
[root@fips-rh6 ~]# ps axf | grep --color=always log4j2.formatMsgNoLookups | grep -v grep
```

```
2364 ?    Sl  3:17 /usr/lib/vmware/viewagent/jre/bin/java -Dlog4j2.formatMsgNoLookups=true -Dfile.encoding=UTF-8 -Djds.folder.preferred=/usr/lib/vmware/viewagent -showversion -Xmx512m
```

Rollback

Connection Server

Editar el siguiente registro:

```
HKLM\Software\VMware, Inc.\VMware VDM\plugins\wsnm\TomcatService\Params\JVMOptions
```

Borrar el siguiente texto y cualquier espacio dentro del valor de registro:

```
-Dlog4j2.formatMsgNoLookups=true
```

Reiniciar el servicio de Connection Server o el equipo

Agente Linux

Dependiendo de la versión de Linux, ingresar en el directorio correspondiente

- `/usr/lib/vmware/viewagent/bin/StartAgent.sh`
- `/etc/rc.d/init.d/viewagent`
- `/etc/init/viewagent.conf`
- `/etc/init.d/viewagent.suse`

Buscar el siguiente texto y eliminarlo

```
-Dlog4j2.formatMsgNoLookups=true
```

Por ejemplo:

Antes: `exec ${exec} -Dlog4j2.formatMsgNoLookups=true -Dfile.encoding=UTF-8`

Después: `exec ${exec} -Dfile.encoding=UTF-8`

Guardar los cambios y reiniciar el servicio de Agente View

```
sudo service viewagent restart
```

Unified Access Gateway

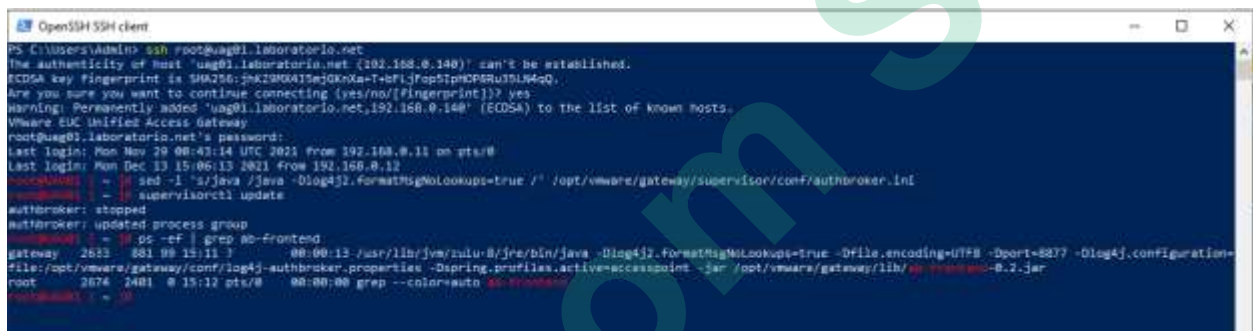
Procedimiento

No existen parches pendientes para los productos afectados. La única solución para remediar las vulnerabilidades consiste en realizar el siguiente workaround.

1. Loguearse como root en la consola del Unified Access Gateway
2. Insertar los siguientes comandos:

```
sed -i 's/java /java -Dlog4j2.formatMsgNoLookups=true /' /opt/vmware/gateway/supervisor/conf/authbroker.ini  
supervisorctl update  
ps -ef | grep ab-frontend
```

3. Verificar que la línea `-Dlog4j2.formatMsgNoLookups=true` esté configurada en true



```
OpenSSH SSH client  
PS C:\Users\Admin> ssh root@uag01.laboratorio.net  
The authenticity of host 'uag01.laboratorio.net (192.168.0.140)' can't be established.  
ECDSA key fingerprint is SHA256:mk23M0M15eJ0kXa-T+FI-JFop5iPhCP8Ru35L3M4gQ.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'uag01.laboratorio.net,192.168.0.140' (ECDSA) to the list of known hosts.  
VMware EUC Unified Access Gateway  
root@uag01.laboratorio.net's password:  
Last login: Mon May 29 08:43:14 UTC 2023 from 192.168.0.11 on pts/0  
Last login: Mon Dec 13 15:06:13 2021 from 192.168.0.12  
root@uag01:~# sed -i 's/java /java -Dlog4j2.formatMsgNoLookups=true /' /opt/vmware/gateway/supervisor/conf/authbroker.ini  
root@uag01:~# supervisorctl update  
authbroker: stopped  
authbroker: updated process group  
root@uag01:~# ps -ef | grep ab-frontend  
gateway 2853 681 09 11:11 ?        00:00:13 /usr/lib/jvm/java-8/jre/bin/java -Dlog4j2.formatMsgNoLookups=true -Dfile.encoding=utf8 -Dport=8837 -Dlog4j.configuration=file:/opt/vmware/gateway/conf/log4j2-authbroker.properties -Dspring.profiles.active=ecssapoint -jar /opt/vmware/gateway/lib/ab-frontend-0.2.jar  
root      2674 2481  0 15:12 pts/0    00:00:00 grep --color=auto ab-frontend  
root@uag01:~#
```

Site Recovery Manager, vSphere Replication

Procedimiento

Site Recovery cuenta con los siguientes appliances - SRM, VR y VRS. Con el fin de mitigar la vulnerabilidad se debe aplicar el hotfix en cada solución de nuestro entorno.

Site Recovery Manager Appliance

Verificar que no existen operaciones "cleanup" pendientes en recovery plans y que tampoco haya errores de configuraciones en la VM que protege Site Recovery Manager.

- Todos los recovery plans se encuentran en estado **Listo**.
- El estado de protección de todos los grupos es **OK**.
- El estado de protección de todas las VMs en los grupos de protección es **OK**.
- El estado de recuperación de todos los grupos de protección es **Listo**.

Conexión al appliance por SSH

En las versiones del appliance 8.3 o mayores debemos asegurarnos que el servicio ssh se encuentre activado para el usuario admin.

Solo se puede habilitar o deshabilitar el acceso por SSH hacia el appliance para el usuario admin.

1. Conectarse a la interfaz del Site Recovery Manager Appliance Management con las credenciales de admin.
2. Dirigirse a Access.
3. En el panel de SSH encontramos la opción para habilitar o deshabilitar SSH.

Es necesario utilizar el usuario de root para facilitar la desactivación de los servicios:

1. Conectarse al Site Recovery Manager Appliance Management por SSH con las credenciales de admin.
2. Correr el comando. su
3. Introducir credenciales de root.

Una vez establecida la conexión con el appliance podremos implementar el workaround:

1. Con el fin de mitigar esta vulnerabilidad necesitamos, como primera instancia, frenar todos los servicios de Java. Para lograrlo se utilizan los siguientes comandos:

```
systemctl stop dr-client.service  
systemctl stop dr-configurator.service
```

2. Mitigar también todos los archivos log4j core jar.

Su automatización puede ser encontrada en "disable_log4j_srm.bash" dentro de la siguiente [KB](#).

3. Realizaremos un SCP (Secure Copy o copia segura) de los archivos hacia la carpeta /root/ utilizando los siguientes comandos en la sesión SSH:

```
chmod +x /root/disable_log4j_srm.bash  
/root/disable_log4j_srm.bash
```

Nota: Puede que figure el siguiente mensaje para cada log4j-core-*-sources.jar zip

"JndiLookup.class not found in /path/to/log4j-core-2.13.3-sources.jar"

Este mensaje corresponde a un comportamiento esperado y por lo tanto es correcto ignorarlo, no será necesario en el presente workaround.

4. Reiniciar todos los servicios Java.

```
systemctl start dr-client.service
```

```
systemctl start dr-configurator.service
```

5. Verificar que la vulnerabilidad fue solventada correctamente.

```
grep -R 'JndiLookup.class' /opt/vmware/
```

Nota: Se espera que el comando no devuelva ningún resultado. En caso de obtener un resultado será necesario volver al paso 1 e implementar nuevamente el workaround.

vSphere Replication Management Server Appliance

Confirmar que no existen ejecuciones activas, las VMs deberán estar en un estado estable; sin errores o en estado de sincronización.

1. Conectar por SSH al appliance de vSphere Replication , el procedimiento para habilitar SSH es el mismo en todas las versiones.
2. Luego, frenar todos los servicios Java. A continuación se detalla el procedimiento por version:

Version 8.5

Será necesario contar con acceso al usuario root con el comando su para detener los siguientes servicios:

```
systemctl stop hms.service  
systemctl stop dr-configurator.service  
systemctl stop dr-client.service
```

Version 8.4

Será necesario contar con acceso al usuario root con el comando su para detener los siguientes servicios:

```
systemctl stop dr-configurator.service  
systemctl stop tomcat.service  
systemctl stop hms.service
```

Version 8.3 – Mitigación con conectivada internet

Ejecutar los siguientes comandos

```
systemctl stop tomcat.service  
systemctl stop hms.service  
dnf install zi
```

Version 8.3 - Mitigación sin conectividad a internet.

Descargar el archivo adjunto de la siguiente [KB](#) y realizar un SCP (Secure Copy o copia segura) de los archivos hacia la carpeta /root/ del appliance por SSH.

Detener los siguientes servicios:

```
systemctl stop tomcat.service
systemctl stop hms.service
rpm --install /root/zip-3.0-2.ph2.x86_64.rpm
```

3. Mitigar también todos los archivos log4j core jar.

Su automatización puede ser encontrada en "disable_log4j_srm.bash" dentro de la KB mencionada anteriormente. Realizaremos un SCP (Secure Copy o copia segura) de los archivos hacia la carpeta /root/ utilizando los siguientes comandos en la sesión SSH:

```
chmod +x /root/disable_log4j.bash
/root/disable_log4j.bash
```

Nota: Puede que nos figure el siguiente mensaje para cada log4j-core-*-sources.jar zip
"JndiLookup.class not found in /path/to/log4j-core-2.13.3-sources.jar"

Este mensaje corresponde a un comportamiento esperado y por lo tanto es correcto ignorarlo, no será necesario en el presente workaround.

4. Reiniciar los servicios del VR según la versión instalada:

Version 8.5

Será necesario contar con acceso al usuario root con el comando su. Ejecutar los siguientes comandos:

```
systemctl start hms.service
systemctl start dr-configurator.service
systemctl start dr-client.service
```

Version 8.4

Será necesario contar con acceso al usuario root con el comando su.

```
systemctl start hms.service
systemctl start dr-configurator.service
systemctl start tomcat.service
```

Version 8.3

Será necesario contar con acceso al usuario root con el comando su. Ejecutar los siguientes comandos:

```
systemctl start hms.service
systemctl start tomcat.service
```

Para validar la afectación de un site recovery appliance podemos correr el siguiente comando desde el usuario root:

```
grep -R 'JndiLookup.class' /opt/vmware/
```

En caso que el comando no devuelve resultado, la mitigación fue exitosa.

vSphere Replication Server (Add-on VR server) Appliance

Confirmar que no existen ejecuciones activas, las VMs deberán estar en un estado estable, sin errores o en estado de sincronización.

1. Conectar por SSH to the vSphere Replication Appliance, el procedimiento para habilitar SSH es el mismo en todas las versiones.
2. A continuación se detalla el procedimiento por version para frenar los servicios:Run the following version specific commands stop the services:

Versión 8.3 - Mitigación con conectividad a internet del appliance.

```
tdnf install zip
```

Versión 8.3 - Mitigación sin conectividad a internet.

Descargar el archivo adjunto del link "zip-3.0-2.ph2.x86_64.rpm" y realizar un SCP (Secure Copy o copia segura) de los archivos hacia la carpeta /root/ del appliance por SSH.

```
rpm --install /root/zip-3.0-2.ph2.x86_64.rpm
```

Versión 8.4 o mayor

Ejecutar el siguiente comando con credenciales de root:

```
systemctl stop dr-configurator.service
```

3. Mitigar también todos los archivos log4j core jar.
Su automatización puede ser encontrada en "disable_log4j_srm.bash" Dentro de la siguiente [KB](#). Realizaremos un SCP (Secure Copy o copia segura) de los archivos hacia la carpeta /root/ utilizando los siguientes comandos en la sesión SSH:

```
chmod +x /root/disable_log4j_srm.bash  
/root/disable_log4j_srm.bash
```

Nota: Puede que nos figure el siguiente mensaje para cada log4j-core-*-sources.jar zip
"JndiLookup.class not found in /path/to/log4j-core-2.13.3-sources.jar"

Este mensaje corresponde a un comportamiento esperado y por lo tanto es correcto ignorarlo, no será necesario en el presente workaround.

4. Reiniciar todos los servicios Java.

```
systemctl start dr-configurator.service
```

5. Verificar que la vulnerabilidad fue solventada correctamente.

```
grep -R 'JndiLookup.class' /opt/vmware
```

Nota: Se espera que el comando no devuelva ningún resultado. En caso de obtener un resultado será necesario volver al paso 1 e implementar nuevamente el workaround.

Validación:

Para validar la afectación de un site recovery appliance podemos correr el siguiente comando desde el usuario root:

```
grep -R 'JndiLookup.class' /opt/vmware/
```

En caso que el comando no devuelva resultado, la mitigación fue exitosa.

NSX-V

Procedimiento

1. Loguearse como admin al NSX Manager vía CLI.
2. Habilitar el modo avanzado con el comando **'en'** e ingresar nuevamente la contraseña de admin.
3. Cambiar a modo root con el comando **'st eng'** y tocar la tecla **Y** para avanzar. Posteriormente, ingresar la contraseña de root **'IAmOnThePhoneWithTechSupport'**
4. Realizar la copia de seguridad de los archivos a modificar:

```
mkdir /root/tanuki-conf  
cp /usr/lib/tanuki/conf/*-wrapper.conf /root/tanuki-conf/
```

5. Ejecutar el siguiente comando para aplicar el workaround:

```
find /usr/lib/tanuki/conf/ -name '*-wrapper.conf' | xargs -n 1 -l {} sh -c 'echo "wrapper.java.additional.100=Dlog4j2.formatMsgNoLookups=true" >> {}'
```

6. Reiniciar el appliance
7. Una vez reiniciado, ejecutar la siguiente captura como root en el NSX Manager:

```
tcpdump -i lo -s 1500 -XX port 389
```

8. Desde otro equipo linux con conectividad hacia el NSX Manager, ejecutar el siguiente comando:

```
curl -H "Content-Type:application/xml" -k -u admin -X POST -d '<securitygroup><name>${jndi:ldap://127.0.0.1/e}</name></securitygroup>' https://<NSX-MANAGER-IP>/api/2.0/services/securitygroup/globalroot-0 reemplazando la IP correspondiente al NSX Manager e ingresando posteriormente la contraseña del usuario admin.
```

9. Si la captura no muestra ningún paquete al ejecutar el curl, el workaround fue aplicado correctamente.

NSX-T

Procedimiento

1. Conectarse a un NSX Manager por SSH, como root.
2. Crear un directorio para guardar un respaldo

```
mkdir /root/tanuki-conf
```

3. Copiar los archivos originales.

```
cp -p /usr/tanuki/conf/*-wrapper.conf /root/tanuki-conf/
```

4. Aplicar el Workaround

```
find /usr/tanuki/conf/ -name '*-wrapper.conf' | xargs -n 1 -I {} sh -c 'echo "wrapper.java.additional.100=-Dlog4j2.formatMsgNoLookups=true" >> {}'
```

5. Reiniciar el appliance

```
/sbin/reboot
```

6. Una vez que se vea que el cluster está estable desde la interfaz gráfica, avanzar con el segundo nodo, incluyendo el reinicio.
7. Una vez que se haya reiniciado el segundo nodo, y el cluster se vea estable, aplicar el procedimiento para el tercer nodo.
8. Verificar que el estado del cluster sea estable.

VCF

Procedimiento

Nota: Estos pasos se aplican a todos los Cloud Builder 3.xy 4.x.

- Asegúrese de que se hayan completado todas las ejecuciones de imágenes y de que no haya ninguna en curso antes de continuar con este procedimiento.
- Inicie sesión en la VM de Cloud Builder
- Ingrese el comando `su` y proporcione la contraseña del usuario `root` para obtener privilegios de super usuario
- Ejecute el siguiente comando para detener el servicio Host Imaging:

```
systemctl stop imaging
```

- Ejecute el siguiente comando para verificar y confirmar que el servicio está detenido

```
systemctl status imaging
```

- Ejecute el siguiente comando para guardar el archivo original antes de editarlo

```
cp /opt/vmware/evorack-imaging/imaging-util-scripts/start-parent-imaging-service.sh  
/opt/vmware/evorack-imaging/imaging-util-scripts/start-parent-imaging-service.sh.orig
```

- Modifique `/opt/vmware/evorack-imaging/imaging-util-scripts/start-parent-imaging-service.sh` para agregar **`-Dlog4j2.formatMsgNoLookups=true`** como un argumento adicional para ejecutar el servicio de imágenes principal en **`"nohup /etc/alternatives/jre/bin/java -jar"`**.

Lo siguiente se da como ejemplo. Asegúrese de que el comando equivalente en el archivo se modifique en consecuencia:

ANTES:

```
nohup /etc/alternatives/jre/bin/java -jar -Dserver.port=$VIA_SERVICE_PORT -  
Dspring.config.additional-location=$VIA_EXTERNAL_PROPERTIES_PATH,$VIA_DB_PROPERTIES_FILE -  
Dserver.servlet.context-path=$VIA_CONTEXT_PATH $VIA_SERVICE_PATH < /dev/null >>$LOGFILE  
2>&1 &
```

DESPUES:

```
nohup /etc/alternatives/jre/bin/java -jar -Dlog4j2.formatMsgNoLookups=true -  
Dserver.port=$VIA_SERVICE_PORT -Dspring.config.additional-  
location=$VIA_EXTERNAL_PROPERTIES_PATH,$VIA_DB_PROPERTIES_FILE -Dserver.servlet.context-  
path=$VIA_CONTEXT_PATH $VIA_SERVICE_PATH < /dev/null >>$LOGFILE 2>&1 &
```

- Ejecute el siguiente comando para guardar el archivo original antes de editarlo

```
cp /opt/vmware/evorack-imaging/imaging-util-scripts/start-imaging-services.sh /opt/vmware/evorack-  
imaging/imaging-util-scripts/start-imaging-services.sh.orig
```

- Modifique /opt/vmware/evorack-imaging/imaging-util-scripts/start-imaging-services.sh para agregar **-Dlog4j2.formatMsgNoLookups = true** como un argumento adicional para ejecutar el servicio de imágenes en "**nohup /etc/alternatives/jre/bin/java -jar**".

Lo siguiente se da como ejemplo. Asegúrese de que el comando equivalente en el archivo se modifique en consecuencia:

ANTES:

```
nohup /etc/alternatives/jre/bin/java -jar -Dserver.port=$SECOND -Dspring.config.additional-  
location=$VIA_DB_PROPERTIES_FILE $name < /dev/null >>$LOGFILE 2>&1 &
```

DESPUES:

```
nohup /etc/alternatives/jre/bin/java -jar -Dlog4j2.formatMsgNoLookups=true -  
Dserver.port=$SECOND -Dspring.config.additional-location=$VIA_DB_PROPERTIES_FILE $name <  
/dev/null >>$LOGFILE 2>&1 &
```

- Ejecute el siguiente comando para confirmar que el servicio Host Imaging está en funcionamiento

```
systemctl start imaging
```

- Ejecute el siguiente comando para confirmar que el servicio está funcionando.

```
systemctl status imaging
```

Nota:

En caso de falla en el inicio del servicio, revierta los archivos de configuración siguiendo los pasos a continuación para activar el servicio y puede comunicarse con el Soporte global de VMware para aplicar los pasos alternativos para mitigar la vulnerabilidad:

- Ejecute el siguiente comando para detener el servicio Host Imaging

```
systemctl stop imaging
```

- Ejecute el siguiente comando para confirmar que el servicio está detenido

```
systemctl status imaging
```

- Copia los archivos originales de nuevo:

```
cp /opt/vmware/evorack-imaging/imaging-util-scripts/start-parent-imaging-service.sh.orig  
/opt/vmware/evorack-imaging/imaging-util-scripts/start-parent-imaging-service.sh  
cp /opt/vmware/evorack-imaging/imaging-util-scripts/start-imaging-services.sh.orig /opt/vmware/evorack-  
imaging/imaging-util-scripts/start-imaging-services.sh
```

- Cambiar los permisos del archivo

```
chmod 755 /opt/vmware/evorack-imaging/imaging-util-scripts/start-parent-imaging-service.sh
```

```
chmod 755 /opt/vmware/evorack-imaging/imaging-util-scripts/start-imaging-services.sh
```

- Reinicie el servicio de imágenes

```
systemctl start imaging
```

- Ejecute el siguiente comando para confirmar que el servicio Host Imaging se ejecuta con la opción **-Dlog4j2.formatMsgNoLookups = true** . La salida debería parecerse a las siguientes

```
ps -ef|grep jar
```

```
root 835 805 7 21:56 ? 00:00:24 /etc/alternatives/jre/bin/java -jar -Dlog4j2.formatMsgNoLookups=true -Dserver.port=8081 -Dspring.config.additional-location=/opt/vmware/evorack-imaging/config/via-db-ext.properties /opt/vmware/evorack-imaging/services/evorack-imaging-services/evorack-imaging-esxi-service-0.0.1-SNAPSHOT.jar
```

```
root 1830 1 10 21:56 ? 00:00:31 /etc/alternatives/jre/bin/java -jar -Dlog4j2.formatMsgNoLookups=true -Dserver.port=8445 -Dspring.config.additional-location=/opt/vmware/evorack-imaging/config/via.properties,/opt/vmware/evorack-imaging/config/via-db-ext.properties -Dserver.servlet.context-path=/via /opt/vmware/evorack-imaging/services/evorack-imaging-services/via.jar
```

```
root 13149 805 99 22:01 ? 00:00:08 /etc/alternatives/jre/bin/java -jar -Dlog4j2.formatMsgNoLookups=true -Dserver.port=8081 -Dspring.config.additional-location=/opt/vmware/evorack-imaging/config/via-db-ext.properties /opt/vmware/evorack-imaging/services/evorack-imaging-services/evorack-imaging-esxi-service-0.0.1-SNAPSHOT.jar
```

```
root 13473 12763 0 22:01 pts/0 00:00:00 grep --color=auto jar
```

Pasos para la automatización de la solución alternativa de Cloud Builder

Siga los pasos a continuación para aplicar la solución mediante un script automatizado

- Inicie sesión en Cloud Builder usando SSH
- Copie el archivo de secuencia de comandos llamado " via_log4j.sh " adjunto en este artículo de KB a su Cloud Builder a través de WinSCP,
 - Copie el archivo al directorio / home
 - NOTA: / tmp puede tener problemas de permisos cuando se ejecuta, así que copie el archivo a / home o cualquier otro directorio
- Cambie el usuario a la cuenta 'root' usando el siguiente comando
 - su -

```
admin@cloud-builder [ ~ ]$ su -
Password:
root@cloud-builder [ ~ ]#
```

- Cambiar el directorio a la ubicación copiada del script

```
cd /hogar
```

- Actualice los permisos del archivo de secuencia de comandos usando el comando 'chmod' que se muestra a continuación

```
chmod 777 via_log4j.sh
```

```
root@cloud-builder [ ~ ]# cd /home/  
root@cloud-builder [ /home ]# chmod 777 via_log4j.sh  
root@cloud-builder [ /home ]# █
```

- Ejecute el script usando el siguiente comando

```
./via_log4j.sh
```

- Una vez que la ejecución del script se completa con éxito, se muestra el siguiente resultado

```
root@cloud-builder [ /home ]# ./via_log4j.sh  
Imaging service stopped successfully  
Imaging service started successfully  
Workaround steps for Cloud Builder Successful  
root@cloud-builder [ /home ]# █
```

Pasos para SDDC Manager

Nota: Estos pasos son aplicables para todas las versiones de VCF 3.xy 4.x Versiones no afectadas VCF 3.10.2, VCF 3.10.2.1 y VCF 3.10.2.2 .

- Inicie sesión en SDDC-Manager usando SSH: `ssh vcf @ <ip / dnsname_of_sddc_manager>`
- Ingrese el comando "su" y proporcione la contraseña del usuario root para obtener privilegios de superusuario
- Haga una copia de seguridad del archivo `/usr/local/vip/bin/start-vip.sh` :

```
cp /usr/local/vip/bin/start-vip.sh /usr/local/vip/bin/start-vip.sh.orig
```

- Modifique el archivo `/usr/local/vip/bin/start-vip.sh` usando el editor "vi":

```
vi /usr/local/vip/bin/start-vip.sh
```

Agregue `-DLOG4J_FORMAT_MSG_NO_LOOKUPS = true` después de `-Djava.compiler = NONE` como el siguiente indicador en la línea (Aprox. Línea 32 col 135)

Lo siguiente se da como ejemplo. Asegúrese de que el comando equivalente en el archivo se modifique en consecuencia

ANTES:

```
nohup $JAVA -jar -Dapp.log.home=/var/log/vmware/vip -server -XX:MaxMetaspaceSize=64m -  
XX:ParallelGCThreads=2 -Djava.compiler=NONE $1 --server.scheme=http --server.http.port=7900>
```

```
$2 2>&1 &
```

DESPUES:

```
nohup $JAVA -jar -Dapp.log.home=/var/log/vmware/vip -server -XX:MaxMetaspaceSize=64m -  
XX:ParallelGCThreads=2 -Djava.compiler=NONE -DLOG4J_FORMAT_MSG_NO_LOOKUPS=true $1 --  
server.scheme=http --server.http.port=7900> $2 2>&1 &
```

- Reinicie el servicio “vip-manager-i18n”

```
systemctl restart vip-manager-i18n.service
```

- Ejecute el siguiente comando para confirmar que el servicio VIP Manager se ejecuta con la opción **-DLOG4J_FORMAT_MSG_NO_LOOKUPS = true** . La salida debería tener un aspecto similar a los siguientes:

```
systemctl status -l vip-manager-i18n.service
```

ANTES:

```
vip-manager-i18n.service - VMware Internationalization Service  
Loaded: loaded (/etc/systemd/system/vip-manager-i18n.service; enabled; vendor preset: enabled)  
Active: active (running) since Sun 2021-12-12 05:00:52 UTC; 16s ago  
Process: 61736 ExecStop=/usr/local/vip/bin/init.sh stop (code=exited, status=0/SUCCESS)  
Process: 61755 ExecStart=/usr/local/vip/bin/init.sh start (code=exited, status=0/SUCCESS)  
Main PID: 61781 (java)  
Tasks: 10 (limit: 19191)  
Memory: 139.4M  
CGroup: /system.slice/vip-manager-i18n.service  
        `-61781 /usr/bin/java -jar -Dapp.log.home=/var/log/vmware/vip -server -  
XX:MaxMetaspaceSize=64m -XX:ParallelGCThreads=2 -Djava.compiler=NONE -  
DLOG4J_FORMAT_MSG_NO_LOOKUPS=true /usr/local/vip/vip-manager-i18n-common.jar --  
vip-service.cross.domain.alloworigin=sddc-manager.vrack.vsphere.local --server.scheme=http --  
server.http.port=7900
```

```
Dec 12 05:00:52 sddc-manager.vrack.vsphere.local init.sh[61755]: start VIP service  
Dec 12 05:00:52 sddc-manager.vrack.vsphere.local init.sh[61755]: execute start function  
Dec 12 05:00:52 sddc-manager.vrack.vsphere.local init.sh[61755]: executing:  
/usr/local/vip/bin/start-vip.sh /usr/local/vip/vip-manager-i18n-common.jar /usr/local/vip/work/vip-  
runtime.log /usr/local/vip/work  
Dec 12 05:00:52 sddc-manager.vrack.vsphere.local init.sh[61755]: =====startup vip=====  
Dec 12 05:00:52 sddc-manager.vrack.vsphere.local init.sh[61755]: found java home:  
/etc/alternatives/jre  
Dec 12 05:00:52 sddc-manager.vrack.vsphere.local init.sh[61755]: run vip from: /usr/local/vip/vip-  
manager-i18n-common.jar  
Dec 12 05:00:52 sddc-manager.vrack.vsphere.local init.sh[61755]: log file: /var/log/vmware/vip/vip-  
runtime.log
```



```
Dec 12 05:00:52 sddc-manager.vrack.vsphere.local init.sh[61755]: vip service is started!  
Dec 12 05:00:52 sddc-manager.vrack.vsphere.local init.sh[61755]: end of starting VIP service  
Dec 12 05:00:52 sddc-manager.vrack.vsphere.local systemd[1]: Started VMware Internationalization Service.
```

Nota: En caso de falla en los pasos anteriores, revierta los archivos siguiendo los pasos a continuación para activar el servicio y puede comunicarse con VMware Global Support para aplicar los pasos alternativos para mitigar la vulnerabilidad:

- Revertir el archivo de configuración

```
cp /usr/local/vip/bin/start-vip.sh.orig /usr/local/vip/bin/start-vip.sh
```

- Cambiar la propiedad y los permisos del archivo

```
chown vcf_vip:vcf /usr/local/vip/bin/start-vip.sh  
chmod 775 /usr/local/vip/bin/start-vip.sh
```

- Reinicie el servicio usando el siguiente comando:

```
systemctl restart vip-manager-i18n.service
```

Pasos para la automatización de la solución alternativa de SDDC Manager

- Inicie sesión en SDDC Manager mediante SSH
- Copie el archivo de secuencia de comandos llamado " **vmsa_log4j_fix.py** " adjunto en este artículo de la base de conocimientos a su administrador de SDDC a través de WinSCP,
 - Copie el archivo al directorio / tmp
- Cambie el usuario a la cuenta 'root' usando el siguiente comando
 - su -

```
vcf@sddc-manager [ ~ ]$ su -  
Password:  
root@sddc-manager [ ~ ]#
```

- Cambiar el directorio a la ubicación copiada del script

```
cd / tmp
```

- Actualice los permisos del archivo de secuencia de comandos usando el comando 'chmod' que se muestra a continuación

```
chmod 777 vmsa_log4j_fix.py
```

```
root@sddc-manager [ ~ ]# cd /tmp/
root@sddc-manager [ /tmp ]# chmod 777 vmsa_log4j_fix.py
root@sddc-manager [ /tmp ]#
```

- Ejecute el script usando el siguiente comando

```
python vmsa_log4j_fix.py
```

- Una vez que la ejecución del script se completa con éxito, se muestra el siguiente resultado

```
root@sddc-manager [ /tmp ]# python vmsa_log4j_fix.py
This script will help to automate the steps described in VMware KB https://kb.vmware.com/s/article/87095#sddc\_manager\_steps
All Services will be restarted by the script to mitigate the VMSA, Please enter YES to proceed further or NO to Exit [[Yes/No/Y/N] ] : YES
Remediating VIP service Config
...Taking Backup of file /usr/local/vip/bin/start-vip.sh
...Successfully completed the backup - /usr/local/vip/bin/start-vip.sh.orig
...Updating Config file
...Reading Config file
...Completed Config file update
...Restart VIP Services
...Successfully re-started VIP Services
...Completed remediating VIP services
...Validating VIP services update
...Successfully validated VIP services update
root@sddc-manager [ /tmp ]#
```

Wetcom S.A.

Identity Manager

NOTA: Se recomienda actualizar las versiones anteriores a versiones compatibles más nuevas antes de aplicar la solución alternativa. Es posible que este procedimiento no funcione para versiones anteriores no compatibles.

Procedimiento

1. Inicie sesión como sshuser
2. Utilice los siguientes comandos para hacer una copia de seguridad y modificar los patrones para configurar % m {nolookups} en lugar de % m en todos los archivos de configuración / propiedades de log4j (ubicados en / usr / local / horizon / conf).

```
cp -r /usr/local/horizon/conf/tmp/conf
sed -i 's /% m /% m {nolookups} /g' /usr/local/horizon/conf/*.*
```

Nota: No ejecute el comando sed más de una vez. Restaure los archivos de / tmp / conf si es necesario.

3. Edite el archivo /opt/vmware/horizon/workspace/bin/setenv.sh
4. Busque la sección " JVM_OPTS = " y busque la siguiente línea de configuración:

```
-Dset.rmi.server.hostname = true \
```

Debajo de esa línea, inserte la siguiente línea nueva y guarde el archivo:

```
-Dlog4j2.formatMsgNoLookups = true \
```

5. Reinicie el servicio horizon-workspace usando el comando. Esto aplicará los cambios realizados en los pasos 2 a 4.

```
service horizon-workspace restart
```

NOTA : Los pasos 6 a 7 son necesarios solo si certproxy para SSO de Android está configurado

6. Modifique los patrones para configurar % m {nolookups} en lugar de % m en /opt/vmware/certproxy/conf/cert-proxy-log4j.properties

Por ejemplo, en VMware Identity Manager 3.3.5, el archivo /opt/vmware/certproxy/conf/cert-proxy-log4j.properties , se realizaría el siguiente cambio:

Antes

```
Appender.rollingfile.layout.pattern original =% d {ISO8601}% -5p (% t) [% X {orgId};% X {userId};% X {ip};% X {executionId}]% c - % m % n Appender.rollingfile.layout.pattern
```

Después

```
=% d {ISO8601}% -5p (% t) [% X {orgId};% X {userId};% X {ip};% X {executionId}]% c - % m {nolookups} % n
```

7. Reinicie el servicio certproxy usando el comando

```
/etc/init.d/vmware-certproxy restart
```

8. Edite el archivo `/opt/vmware/elasticsearch/config/jvm.options` si está presente en el sistema. De lo contrario, puede omitir los pasos 8-10.

9. Busque la sección "`# log4j 2`" y busque la siguiente línea de configuración:

```
-Dlog4j2.disable.jmx = true
```

Debajo de esa línea inserta la siguiente configuración y guarda el archivo:

```
-Dlog4j2.formatMsgNoLookups = true
```

10. Reinicie el servicio elasticsearch usando el comando

```
service elasticsearch restart
```

Alternativamente, use el script adjunto log4j.sh para realizar cambios

1. Descargue el archivo `log4j.sh` de la siguiente [KB](#) y scp en el directorio `/tmp` del dispositivo
2. Inicie sesión en el dispositivo como `sshuser`, sudo al acceso de nivel raíz
3. Cambiar al directorio `/tmp`

```
cd /tmp
```
4. Ejecute el siguiente comando para que el script `log4j.sh` sea ejecutable:

```
chmod +x log4j.sh
```
5. Ejecute el siguiente comando para ejecutar el script:

```
./log4j.sh
```

Tanzu Kubernetes

Procedimiento

1. Deshabilite la resurrección de VM de BOSH en la VM de PKS-API "pivotal-container-service / *" que ejecuta UAA, para evitar la reversión de estos cambios.

Nota: Consulte <https://bosh.io/docs/resurrector/>

2. Obtenga acceso a la línea de comandos de BOSH mediante SSH en el Administrador de operaciones, como se documenta aquí: <https://docs.pivotal.io/ops-manager/2-7/install/trouble-advanced.html> .
3. Escribe el siguiente guión

```
#!/bin/bash

set -u -o pipefail

# Update script for UAA

file=/var/vcap/jobs/uaa/bin/uaa

grep -q '^JAVA_OPTS="$JAVA_OPTS -Dlog4j2.formatMsgNoLookups=true"' "$file"

status=$?

if [ "$status" -gt 1 ]; then

    echo grep error 1>&2

    exit 1

fi

if [ "$status" -eq 1 ]; then

    set -e

    new="$(set -euo pipefail; awk '/JAVA_OPTS="[^$].*$/ {print;print "JAVA_OPTS=\"$JAVA_OPTS -Dlog4j2.formatMsgNoLookups=true\"";next}1' $file)"
```

```
if [ "$?" -ne 0 ]; then

echo awk error 1>&2

exit 1

fi

echo "$new" > "$file"

fi

# Update script for pks-api

sed -i "s/java -Dspring.config.location/java -Dlog4j2.formatMsgNoLookups=true -Dspring.config.location/g"
/var/vcap/jobs/pks-api/bin/pks-api-ctl.sh

# Restart UAA and pks-api

monit restart uaa

monit restart pks-api
```

Copie el script anterior en pks-api VM usando el siguiente comando:

```
bosh -d pivotal-container-service-2162097b3a142fdc32bb scp tkgi-
mitigation.sh pivotal-container-service: / tmp /.
```

Ejecute el script usando el comando a continuación,

```
bosh -d pivotal-container-service-2162097b3a142fdc32bb ssh pivotal-
container-service -c 'sudo bash / tmp / tkgi-mitigation.sh '
```

Nota: Cuando la solución / parche a largo plazo esté disponible, habilite la resurrección de BOSH.

Links de referencia

<https://www.vmware.com/security/advisories/VMSA-2021-0028.html>

Wetcom S.A.