Workaround de CVE-2021-44228 en vRealize Automation 8.x y vRealize Orchestrator 8.x

Según un comunicado emitido por el fabricante VMware el **15/12** se detectó **una** vulnerabilidad. Los CVEs de las mismas son: **CVE-2021-44228**

Estas vulnerabilidades fueron informadas **pública** a VMware. Se encuentran workarounds disponibles para remediar las vulnerabilidades en los productos afectados:

- vRealize Automation
- vRealize Orchestrator

¿Cómo me afecta?

vRealize Automation y vRealize Orchestrator utilizan Apache Log4j, la cual es una herramienta de captura de logs basada en Java. Con ciertas funciones de Apache Log4j, es posible construir solicitudes maliciosas que desencadenan en vulnerabilidades de ejecución remota de código.

¿A quiénes afecta?

Los productos afectados son vRealize Automation 7.6 y 8.x y vRealize Orchestrator 7.6 y 8.x

Nota: En el caso que se haya aplicado los workarounds previo al **15 de diciembre**, se deberán volver a ejecutar para asegurarse de tener los últimos fixes. En el caso que se tenga un vRealize Automation 7.6 con un vRealize Orchestrator 7.6 embebido, se deben realizar los pasos 3 y 4. Caso contrario, estos pasos deben ser exceptuados.

Resolución

vRealize Automation 7.6 (Pasos 3 y 4 para vRealize Orchestrator embebido)

- Realizar Backup de todos los nodos

Procedimiento

1. Conectarse por SSH a **cada uno** de los nodos para ejecutar los siguientes pasos
2. Parar el servicio **vco-configurator** en **cada uno** de los nodos con el comando:

   service vco-configurator stop

3. Ejecutar el siguiente comando en cada uno de los nodos:

base64 -d <<<
"bG9nX21lc3NhZ2VfbG9nNGooKSB7CiAgZWNobyAiWyQoZGF0ZSAtLXV0YyAiKyVGVCVULiUzTloiKV0gJDEiI
HwgdGVlIC1hIC92YXIvbG9nL3Ztd2FyZS92Y28vYXBwLXNlcnZlci92Y29fbG9nNGpfY3ZlLmxvZwp9Cgpsb2dfZ

XJyb3JfbG9nNGooKSB7CiAgbG9nX21lc3NhZ2VfbG9nNGogIkVSUk9SOiAkMSIKICBleGl0IDEKfQoKdXBkYXRl
X3Zyb190b21jYXRfc3RhcnQoKSB7CiAgbG9jYWwgZmlsZT0iJDEiCiAgbG9nX21lc3NhZ2VfbG9nNGogIk1vZGl
meWluZyB2Uk8gdG9tY2F0IHN0YXJ0dXAgY29uZmlnIC0gJGZpbGUiCgogIHJlcz0kKGF3ayAnRk5SPT1OUnsg
aWYgKC9eZXZhbCBleGVjLykgcD1OUjsgbmV4dH0gMTsgRk5SPT1weyBwcmludCAiSTJ4dlp6UnFYMk4yWlY
5M2IzSnJZWEp2ZFc1a0NteHZaMTl0WlhOellXZGxYMnh2WnpScU1sOWpkbVVvS1NCN0NpQWdaV05vYnlB
aVd5UW9aR0YwWlNBdExYVjBZeUFpS3lWR1ZDVlVMaVV6VGxvaUtWMGdKREVpSUFwOUNncHdZWFJqYU
Y5d2JIVm5hVzRvS1NCN0NpQWdJQ0JzYjJOaGJDQndiSFZuYVc1ZmNHRjBhRDBpSkRFaUNpQWdJQ0JzYjJOa
GJDQjBaVzF3WDNCaGRHZzlMM1J0Y0M4a0tHSmhjMlZ1WVcxbElDUndiSFZuYVc1ZmNHRjBhQ2tLSUNBZ0l
HeHZZMkZzSUdKaFkydDFjSE5mY0dGMGFEMGlMM1Z6Y2k5c2FXSXZkbU52TDJKaFkydDFjSE1pQ2dvZ0lDQ
WdiV3RrYVhJZ0xYQWdKR0poWTJ0MWNITmZjR0YwYUFvS0lDQWdJSEp0SUMxeVppQWtkR1Z0Y0Y5d1lYU
m9DaUFnSUNCMWJucHBjQ0F0Y1NBa2NHeDFaMmx1WDNCaGRHZ2dMV1FnSkhSbGJYQmZjR0YwYUNCO
GZDQmxlR2wwSURFS0lDQWdJQW9nSUNBZ0l5QkRhR1ZqYXlCcFppQjBhR1Z5WlNCcGN5QmhJRzVsWldRZ
2RHOGdkWEJrWVhSbElIUm9aU0J3YkhWbmFXNEtJQ0FnSUdsbUlHWnBibVFnSkhSbGJYQmZjR0YwYUNBd
GVHUmxkaUF0ZEhsd1pTQm1JQzF1WVcxbElDZHNiMmMwYWkxamIzSmxMVElxYW1GeUp5QXRaWGhsW
XlBdmRYTnlMMkpwYmk5NmFYQWdMWE5tSUh0OUlGdzdJSHdnWjNKbGNDQnZjbWN2WVhCaFkyaGxM
Mnh2WjJkcGJtY3ZiRzluTkdvdlkyOXlaUzlzYjI5cmRYQXZTbTVrYVV4dmIydDFjQzVqYkdGemN6c0tJQ0FnSUhS
b1pXNEtJQ0FnSUNBZ0lDQnNiMmRmYldWemMyRm5aVjlzYjJjMGFqSmZZM1psSUNKTmIyUnBabmxwYm1j
Z2NHeDFaMmx1T2lBa0tHSmhjMlZ1WVcxbElDUndiSFZuYVc1ZmNHRjBhQ2tpQ2lBZ0lDQWdJQ0FnYlhZZ0pI
QnNkV2RwYmw5d1lYUm9JQ1JpWVdOcmRYQnpYM0JoZEdnS0lDQWdJQ0FnSUNCbWFXNWtJQ1IwWlcxd1
gzQmhkR2dnTFhoa1pYWWdMWFI1Y0dVZ1ppQXRibUZ0WlNBbmJHOW5OR290WTI5eVpTMHlLbXBoY2ljZ
0xXVjRaV01nYzJnZ0xXTWdKeTkxYzNJdlltbHVMM3BwY0NBdGNTQXRaQ0I3ZlNCdmNtY3ZZWEJoWTJobEw
yeHZaMmRwYm1jdmJHOW5OR292WTI5eVpTOXNiMjlyZFhBdlNtNWthVXh2YjJ0MWNDNWpiR0Z6Y3pzZ2
RHOTFZMmdnTFhRZ01qQXlNVEF4TURFd01EQXdJSHQ5SnlCY093b2dJQ0FnSUNBZ0lDaGpaQ0FrZEdWdGN
GOXdZWFJvSURzZ2VtbHdJQzF4SUMxeUlDMVlJQzFFSUNSd2JIVm5hVzVmY0dGMGFDQXFLU0l4ZkNCbGVH
bDBJREVLQ2lBZ0lDQWdJQ0FnSXlCR2FYZ2djbWxuYUhSekNpQWdJQ0FnSUNBZ1kyaHZkMjRnZG1Odk9uW
mpieUFrY0d4MVoybHVYM0JoZEdnS0lDQWdJQ0FnSUNCamFHMXZaQ0F3TmpRMElDUndiSFZuYVc1ZmNH
RjBhQW9nSUNBZ0lDQWdJR3h2WjE5dFpYTnpZV2RsWDJ4dlp6UnFNbDlqZG1VZ0lsTjFZMk5sYzNOObWRXeH
NlU0J3WVhSamFHVmtJSEJzZFdkcGJqb2dKQ2hpWVhObGJtRnRaU0FrY0d4MVoybHVYM0JoZEdncElnb2dJQ
0FnWld4elpRb2dJQ0FnSUNBZ0lHeHZaMTl0WlhOellXZGxYMnh2WnpScU1sOWpkbVVnSWs1dmRHaHBib
WNnZEc4Z1pHOGdabTl5SUhCc2RXZHBiam9nSkNoaVlYTmxibUZ0WlNBa2NHeDFaMmx1WDNCaGRHZ3BJ
Z29nSUNBZ1pta0tJQ0FnSUhKdElDMXlaaUFrZEdWdGNGOXdZWFJvQ24wS0NuQmhkR05vWDJGc2JGOXdiS
FZuYVc1ektDa2dld29nSUNBZ1ptOXlJR1pwYkdVZ2FXNGdMM1Z6Y2k5c2FXSXZkbU52TDJGd2NDMXpaWEo
yWlhJdmNHeDFaMmx1Y3k4cUxtUmhjZ29nSUNBZ1pHOEtJQ0FnSUNBZ0lDQndZWFJqYUY5d2JIVm5hVzRn
SWlSbWFXeGxJaUI4ZkNCc2IyZGZiV1Z6YzJGblpWOXNiMmMwYWpKZlkzWmxJQ0pGVWxKUFVqb2dSbUZw
YkdWa0lIUnZJSEJoZEdOb0lIQnNkV2RwYmpvZ0pDaGlZWE5sYm1GdFpTQWtabWxzWlNraUNpQWdJQ0JrYjI
1bENnb2dJQ0FnYkc5blgyMWxjM05oWjJWZmJHOW5OR295WDJOMlpTQWlVR0YwWTJocGJtY2daRzl1Wl
M0aUNuMEsifCJiYXNlNjQgLS1kZWNvZGUifScgJGZpbGUgJGZpbGUpIHx8IGxvZ19lcnJvcl9sb2c0aiAiRmFpb
GVkIHRvIGVkaXQgJGZpbGUiCiAgZWNobyAiJHJlcyIgPiAkZmlsZQoKICByZXM9JChhd2sgJ0ZOUj09TlJ7IGlmIC
gvXlx0K2FjdGlvbj0ic3RhcnQiJC8pIHA9TlI7IG5leHR9IDE7IEZOUj09cHsgcHJpbnQgIlx0XHRcdHBhdGNoX2Fsb
F9wbHVnaW5zID4+IC92YXIvbG9nL3Ztd2FyZS92Y28vYXBwLXNlcnZlci92Y29fbG9nNGpfY3ZlLmxvZyAiIH0nI
CRmaWxlICRmaWxlKSAmJiBsb2dfbWVzc2FnZV9sb2c0aiAiU3VjY2Vzc2Z1bGx5IG1vZGlmaWVkIHRoZSB2Uk
8gdG9tY2F0IHN0YXJ0dXAgY29uZmlnIC0gJGZpbGUiIHx8IGxvZ19lcnJvcl9sb2c0aiAiRmFpbGVkIHRvIGVkaXQ

gJGZpbGUiCiAgZWNobyAiJHJlcyIgPiAkZmlsZQoKICBzZWQgLWkgJy9sb2c0al9jdmVfd29ya2Fyb3VuZCA+L2
QnICRmaWxlIHx8IHRydWUKfQoKCnVwZGF0ZV92cm9fdG9tY2F0X3N0YXJ0ICIvdmFyL2xpYi92Y28vYXBwLX
NlcnZlci9iaW4vaW5pdC5kLnNoIiB8fCBsb2dfZXJyb3JfbG9nNGogIkZhaWxlZCB0byBhcHBseSB0aGUgbG9n
NGogQ1ZFIHdvcmthcm91bmQgZm9yIHZSTy4gRm9yIG1vcmUgZGV0YWlscyBzZWUgL3Zhci9sb2cvdm13YX
JlL3Zjby9hcHAtc2VydmVyL3Zjb19sb2c0al9jdmUubG9nLiI=" | sh -

4. Ejecutar el siguiente comando para actualizar vRO Controler Center en cada nodo:

   /usr/lib/vco/tools/configuration-cli/bin/vro-configure-inner.sh controlcenter-update

5. Correr el siguiente comando para actualizar la configuración de vRA y vIDM en cada nodo:

base64 -d <<<
"bG9nX21lc3NhZ2UoKSB7CiAgZWNobyAiWyQoZGF0ZSAtLXV0YyAiKyVGVCVULiUzTloiKV0gJDEiIHwgdGVlI
C1hICAgL3Zhci9sb2cvdm13YXJlL3ZjYWMvdmNhY19sb2c0al9jdmUubG9nCn0KCmxvZ19lcnJvcigpIHsKICBs
b2dfbWVzc2FnZSAiRVJST1I6ICQxIgogIGV4aXQgMQp9CgpkZWxldGVfam5kaV9jbGFzcygpIHsKICBsb2dfbW
Vzc2FnZSAiRGVsZXRpbmcgYWxsIEpuZGlMb29rdXAuY2xhc3MgZmlsZXMgZm91bmQgZm9yIGxvZzRqIDIue
CB2ZXJzaW9ucyIKICBmaW5kIC8gLXhkZXYgLXR5cGUgZiAtbmFtZSAnbG9nNGotY29yZS0yKmphcicgLWV4Z
WMgL3Vzci9iaW4vemlwIC1xIC1kIHt9IG9yZy9hcGFjaGUvbG9nZ2luZy9sb2c0ai9jb3JlL2xvb2t1cC9KbmRpT
G9va3VwLmNsYXNzIFw7IHwgdGVlIC1hIC92YXIvbG9nL3Ztd2FyZS92Y2FjL3ZjYWNfbG9nNGpfY3ZlLmxvZwp
9CgpkZWxldGVfam5kaV9jbGFzcyB8fCBsb2dfZXJyb3IgIkZhaWxlZCB0byBhcHBseSB0aGUgbG9nNGogQ1ZFI
Hdvcmthcm91bmQgZm9yIHZSQS4gRm9yIG1vcmUgZGV0YWlscyBzZWUgL3Zhci9sb2cvdm13YXJlL3ZjYWM
vdmNhY19sb2c0al9jdmUubG9nLiI=" | sh –

6. Reiniciar los siguientes servicios en cada nodo:
   a. *service horizon-workspace restart && base64 -d <<<*
      "IyEvYmluL2Jhc2gKZWNobyAnV2FpdGluZyBmb3IgaG9yaXpvbiBzZXJ2aWNlIHRvIHN0YXJ0
      Li4uJwpmb3IgaSBpbiB7MS4uMTIwfQpkbwogICBzdGF0dXNfY29kZT1gY3VybCAtLW1heC1
      0aW1lIDMwIC1vIC9kZXYvbnVsbCAtcyAtdyAiJXtodHRwX2NvZGV9XG4iICdodHRwOi8vbG9j
      YWxob3N0OjgwODAvU0FBUy9BUEkvMS4wL1JFU1Qvc3lzdGVtL2hlYWx0aCdgCiAgIFtbICI
      ke3N0YXR1c19jb2RlfSIgPT0gIjIiKiBdXSAmJiBicmVhawogICBlY2hvICJIb3Jpem9uIGlzIHN0a
      WxsIHN0YXJ0aW5nLi4uIgogICBzbGVlcCA1CmRvbmUKCmlmIFtbICIke3N0YXR1c19jb2RlfSI
      gPT0gIjIiKiBdXTsKdGhlbgogICBlY2hvICdIb3Jpem9uIHNlcnZpY2Ugc3RhcnRlZCBzdWNjZXNz
      ZnVsbHkhJwplbHNlCiAgIGVjaG8gJ0hvcml6b24gc2VydmljZSBkaWQgbm90IHN0YXJ0IHdpd
      GhpbiB0aGUgZXhwZWN0ZWQgcGVyaW9kLiBDaGVjayBzdGF0dXMgb2YgaG9yaXpvbi13b
      3Jrc3BhY2Ugc2VydmljZSBhbmQgbG9ncyBpbiAvdmFyL2xvZy92bXdhcmUvaG9yaXpvbi8gZ
      m9yIG1vcmUgZGV0YWlscy4nCiAgIGV4aXQgMQpmaQo=" | sh –
   b. *service elasticsearch restart*
   c. *service vco-server status | grep PID && service vco-server restart*
   d. *service vco-configurator start*
      service vcac-server restart

7. Para validar que el workaround haya sido exitoso seguir los siguientes pasos en cada uno de los nodos:
    a. Revisar el log */var/log/vco/app-server/vco_log4j_cve.log* hasta que se vea 'Patching done.'
    b. Correr el siguiente comando para verificar que **JndiLookup.class** no esté presente en ningún archivo de log4j jar para versiones de 2.x. Este no debe devolver ningún output: *find / -xdev -type f -name 'log4j-core-2*jar' -exec sh -c '/usr/bin/unzip -l "{}" | grep org/apache/logging/log4j/core/lookup/JndiLookup.class' \;*

Método de Rollback

- Restaurar los backups

vRealize Automation 8.x y vRealize Orchestrator 8.x:

- Se debe tomar snapshot sin memoria de todos los nodos del cluster

Procedimiento

1. Conectarse por SSH a **un nodo**
2. Ejecutar el siguiente comando: *vracli cluster exec -- sh -c "current_node" && vracli cluster exec -- sh -c "base64 -d <<< '/Td6WFoAAATm1rRGAgAhARwAAAAQz1jM4NCtD5NdADmZSuojhr8q8RskPKwtrPJnfeTy62+4gkp6IAHJt7z/IAlAE34mhHeD+aO6hKL4FKnH1FFyuQkQAbIkb9+Jxr/mBShPT+kQIqQgJ9uUA9aVcJkEH2LD5FcwKUc+AOzrUnv2eW7IAa2JTxxI+m3RAei3iHxpOmeUl5vgMKmFEdTrdmQxEM2j7KGwO9cAM4E4NkBbaru+xfKmjzDfY3KVQYDhYB9vASv6vT+KmikoprMsfrjpd51jMF6G6coW+X9FRZGiDWQOBQgn8nwVxNO7dXYEJdsrIaNfqtN6naau6MGNAOgWD7/xcQ3zSVAE4dXwe2n4FAUjB9KfewJggCJAepRN9ppgQz2U1WyNnLHjgW0eQR+fhZiv/fCzJ1F16Iic2pFaf26TwiMwTsuIPTK57CmRKPa8slW6fN2fpkmm/IAQmhIkwnM/8wn9KDP5bR2p+zAxSOc9Zn9PKl4f0Dk2ECiki8regEx0UGzvxdIeKVkxnLrgLInu7JH9IFCa3lahubQIIAmC3gz5Akf1Dzb4e0IpjOOyYpqKZvJaC3ewR2OvFQN/0F+iyh6LuAdWf1mjJf7BhvfMGlT0Ypyt/1PS3BPhO9rqEaaSz3IOiJ4EPPu719fyEn3jQmc+eQfmbgGNFW06PwfRAndqoX+kMztFD5gG4qFDKL5KYAMid35N3FxGfmZkHB0hOGNagR40ESqy48DqRFTEYs8lAbnb2KRpKgHFNwdbsmHUJgx1T7YY5jiWd/mDCEr1pxBQDiKUrCPRTRWQAZPM5uFuOsjhjVbQNLLU8jeWfRX9LmWTznscGDNXSWmU4hrK9gENMfN4sh2x94Gad4GfG8I2j+czsAOcrIFYDpEpM0lePYoD9UmJIP+nw5jpiIojnAdX8BKwXsVnb13rUs+XsFW0M8q9QPUfJwhhjZohv8ca+7lBKGHWg0DAMWu/QVu4H/ZYdwv2jEe+q1h7mLAj2vN+j49VR5zy8In10Cg5hOOT0DnZT5UgwVG8c2rtZUOrpNwee02wnp+ctz9xmvzU1p9/9xwnPgmez/jUFZbt6kEKjgZ0SS/Ozh/rqNfvsHy2Z/bYcoZrVhrbf/6gsLgLkmb7rKvJauX7VmcaNPRXwo+Bf+jBrsazP5IRiHfrMNh+j+1I3Px/gJv/XPuMF7mYw2Jhhy0lgoM4QIvhlvlEtyT/rW4pFzIWnAKAETOWHv4ZabfeVP3QtU/RKA3pVeunjZNciprSItFIerNSvFnjY2ruitGWh+19Atr/ZdPS0Fb0fsItGU9GYwC/AeO*

wUYk+2AyNnXp9mLN8wm69gidCfPpxJq2jqfVrA3QkXP9/DfESQQimuAiqHqVgo581OUNf0D2IZfeH
Z6Rc7OpraoTt0c7ETiyLC+CdxBzXmlmG8oXHGXN44+5H2dnuhPT1RjFKZ3wujExZnP6dsMKldrD3LAf
l5C9X6ZjKTmt69nmW5CqCByQu0FRZIMu0UtbJaW+wucWWqMWXSLa6JiJiVIpTgaQeP2AQ5HYbR5
qyioDrye2wcwQtvgxuBk047tFxkenOFhk0zfH6hYUSga1FZQg+zGHY4DCq0gvriXnCJmLiMgggS1RfPJ
ALXM7FyoDViGnNjsm7y/KNzjA5beAzQfHvLEruZyXeXcUBYWrT8twc7rjKQ+i51hOCcGF6bJE5ipxSI+
O5WDRlKNl1zjY86P1Wou9hNKDojiGuL8ga8+C+pF5ZuFvdgZbhTcPHeORxuWVx925OKFL+AmKn+P
dgEkZf8AoR0t5W3Ktl5EgmUMLpL5djgNVY4Z5vPckGc+qLsGWuSmxBgj8Z4/yxKepbab52z6J2I6vL6
ps1fFypLIIO1DHo6YRPcgt+lpPEFyVHZ3hhZGQg+SGvsLTl7Z8L8IWaL4m94U3Q/YhVtq+VN9EOsh10
/gh6bYrSNnwYao6OQSJ/u/K3Z65+aUWmjbcoQ+ueilYxuM/XEnM2IxNk0TfY11cCGd/pprku/MRtV+i
Y0csvCF5tof7dbreX88MeYnIUsSAkFQlpNDlWg5uOhTKNy3pkBDs7zbw22TW/3dH4zEPY0S3zlHWM
KKYB7nU2ody+suadMUx0nk1mHv5cUvWtFN7oQUwwTew8fWvG3oGEcijAwMbLZ1lx3BsjqiFHanz
AOSvTJ3oXlpL81yFY6W4ONdz869yHJn5ZDqoopWyCt/LKK78NCztVM+lQg0QUHNOG6Yg0po48Xfs
QopwYLKeIHrpivLqcv+47ajWd68BT9KwtKob+GuxVdpwC97l5KRJw8Koom/wJ0XBBMbI/MpXVcM+j
1olmk8hd/egBpLW8fbNr+hBxKRgHmWDRHmnZArM0Jt5U7I6507OqjPJupqDgRs18JKxEQE6+DY5v
xmYymm8qSP9wkNz1XWar0GJP4HyFQOD9HJ4YnRw24/rZSwFvr2c1V1QC2y1Y9aFdrRr85ho5obFc
k35td2ujfoeYyWT7SPcszZun1UuVCU9D3BYESmu6k0F4O6E23YuPQzbqJHcVjae24VZ+VlUbvf1HPI8
xXoUPlOYUuqoE+NFaUVq7BF6vIN7tmWEQlBk8Sy9lESm+SjZ0eGpAwi7K+dTzhJjQ8aOz6kJTgqNahy
FVhdTigrtRCtOrq/IYMaEG/XhVocPpiE6Ci4g81NCKMdrrWmD6WOByKOdZfNLnhB5BFKPtvGu+jOw
AqIBNDecpt/ZqxeOCE4OEuAblci7/5GU2hjFse2SjfZQnbM9c1VuxaGtU/8XUxA6TSNCNHRHMvvCU2
s+YA6ctz/QkSmbQ5Ma3zj4dkU6sqwugsHX1bRuRDP/9yT57VwMB11U9SVnhXWHYHvrziU0lzbFszC
ayC36Wrr/TfyCyvkEGP+o9lKsnvqfA5Hw35kZUQM0aXFJGSnrhqPZKuvnXPsBtWPByjLmJmZtLqSOW
SDCJm6/RjksWL7yvhYuerbIQ9xBpAew0pF/6l/6LMh+Wj1vG5FygkiJ75ut2mv9GPFmprf+jfyGaII3wx
SdEZKigktvs6bMIGSPHI+4/xRiMelge90UNKtnIFzAIJ6xGrAkBQH568evD9c6eWGXDTWylYTjzd3U1H
R3pV4K/tjC01JdUDZLgewX82I7Kiehjp38nTsW0zYmAvV7NPtrohU8N6t2FEUY1w6fffHRK2vRUZBHV
urPiDNopLs1GusHHSlR9rqUqQXz1Au773w9nfNXUiXsCgphVHYTpMPDgCZv/g+J3z8htkydYt3xadV0
8PCs709L65idOeG5oQ6akvenE82xQzitbp9K9IUPwZRp+Ll21mmfXAr7adPAZLiTRt9pq7NjqbF2eCn+
msPj1ltXXDuT09beUavLbjlBIRzAqZICC1kBe9MNEDxBwVHn9Y7RnXnbRf2XSf93e+q1YLwk3u06FiF
UgkEMGAH4UlE4uzbF2tzkMQWa6xWnRB6rRAlUiNKYK0g+CRRdifCrm0ZAdyUoEbijorGzYU0vPd4a
NFH2ZnnuuSpY7yMwF0XwOeLiAFUhMRqujjJbAFFnGCMoJDSgYTvbLQRWSKZOYKNK2WtyGQQguL
LZ0Kv7neWe5d6bSvYlIR3V9Px3c8F9hdNRc2O9FcYjyotJE5Oo4o1MiLJRLCSzYbQ8YTihivtEtQmtBMI
ZcH799T4WbwCrn//bb6sdjSc5AeA5gAppi63mQlCXIfDYuu4C29eriKRoP5y/Aa5KK4Y2loJOixuR1Rh
qLh3LefcCankhEQ7y+7zREaniU2BiRNgOHPVfxesSNd9lNQlgmcAv86A5rEUNv3EZPDxi5yqNcfLuXW
lKjNpcfylURWc9MJlXNmJyb2QvTWhJGy8GXieN+WOUapLiN3b8GDgMncC6SydTVHjcHEOOmw5fb
7akGk8rAfu1ZZsNC4yY49J+PJehCQ5rAHunDwzgPqnNECjdXgFSWVMGApFu9iYE0/DYrdrvVDvIpbDj
ZYxKbn0+vA/KXx/ogj04qD12Txl1zEsVW0SFiFlCWj7KPoTALQ1kzrgeqTtpEwXjWtPW/V4iPSHNPS38
A9+V/Uc2GWOwl0CLLqiffkeZ0OWswUJ/Dk5oYMVn1QT1kI3KEB4RXvwKTe/V+0XXEpalMCbIj8asFI
sxG6+vmGGlTw/yCB8qhRgr/EbGJWb2RQb43gRcgfAA3+dHhh1eExHG/zLpqLMUomktCAFk24fviW
Ep2OifH/6G+nSQeaodsbfMoToZKO71YuouVdyZqiRfxPskBMg23xE9b6Kzb5k86mbMW4dYD4mram
fEJ4PbZpaR49is9eDDnc3J+DaTy5iJmvwBoaWHStq10gVweLExLw+LWEp3xn1dD6ptv18Np2Osi597
nB42a0bJ7bVZk5zko84tZoS4Opt8fn5BJlNnxq4PBSNQbmamsSe+3kWw9BOzrDOUuDTYH9oXLVtk
wFl+7rRPLgNY7FA50YDIWmhMxJNJWzQvGhcmgDGTGR8Suj3O0mavs6o56Hj3p78iNpC4C6/GQQ
YjHufaik7mcBck1M8ShgZh5pqkdW7duCCvSOSTDfXez5S3INEw06NDVxysd6bG9gmEmEhXVdlUK6

1UY9eThmU7L0qSDdnCqaauFIEPn3NnPT2g/1yfgYJordkDBetOgzXkLy/c1VY9N5vhJKgK+NwMWqUdYkSCi6q/7yJib7vyiTzAd66MjI/lXRlQmRnn3PX5nXo5brrkQFJk+XnuLaSst0B8D309QWb16cHyFnciiS9tCGVDffe0IQvKT0uSGLAtIdUHAmpX+rSgoaiETbIENBvo8egh7epr4hcbxdSJY+m1mOWK/MIVCuie4Vg0LhCwIWxCGXuHLTXamClEJrta6jvlqJJPeYDdwO3NpTCHw7DrQhMc8smEDofPoSmxnAB2CwIPyt64B3Y1Ju/Y00TGqPJcUekOuMK5I1CPqFRdJNqAe337ulmTJUwpoDuZQq8Sftz/Gi34NC31YBYWgKrrHl8ZySS5G2eqKoZ6ARNyU9m5mJainJUDaqWW6QmRxrJ8c1570cmWDyP3aoiML9XsrjG2HxXeI8V4SixYb+zRgjjsJ7kd5K+KuSRcs7D5zbhzxV/RWYlltBUTF3RvYxECisSgl0HWFQwKWDUz92S49tmp8ui9sBCulK2FxvUdZCER/ZN3hXu5rSjvai05qHZQxhqdn/r1NyRjk/zGAH/7FPtAJOUrPZOS5VqGSy1A6ij5hoo5CXUC5m5ypx+rMEh2mxkGeb4HHtbQaJI7QG0bO8uPx3SNQjLLV4bOb30VUkVxM7ljKw/va/P5c6HxyS7jrUQGqHlprRCHA19lUUuWvOW/ZiayKNGbDwfWm4USXhtoyvlMKWCv4AAAAAhiZwz+MqZEAAa8frqEDABd9jJexxGf7AgAAAAEWVo=' | xz -d | bash -" && vracli cluster exec -- /etc/bootstrap/postupdate.d/71-15-cve-2021-44228.sh

3. Ejecutar el script con el comando */opt/scripts/deploy.sh*
4. Para validar que el script haya corrido correctamente, se debe ejecutar el siguiente comando y verificar que no devuelva nada: */opt/scripts/deploy.sh*

Método de Rollback

- Revertir las snapshots

vRealize Orchestrator 7.6 (Para una instancia externa a vRealize Automation)

- Tomar backup de todos los nodos

Procedimiento

1. Conectarse por SSH a cada nodo y seguir los siguientes pasos
2. Parar el servicio **vco-configurator** en cada nodo con el comando: *service vco-configurator stop*
3. Ejecutar el siguiente comando para actualizar la configuración de vRO en cada nodo:

base64 -d <<<
"bG9nX21lc3NhZ2VfbG9nNGooKSB7CiAgZWNobyAiWyQoZGF0ZSAtLXV0YyAiKyVGVCVULiUzTloiKV0gJDEiIHwgdGVlIC1hIC92YXIvbG9nL3Ztd2FyZS92Y28vYXBwLXNlcnZlci92Y29fbG9nNGpfY3ZlLmxvZwp9Cgpsb2dfZXJyb3JfbG9nNGooKSB7CiAgbG9nX21lc3NhZ2VfbG9nNGogIkVSUk9SOiAkMSIKICBleGl0IDEKfQoKc2V0X2phdmFfb3B0KCkgewogIGxvY2FsIGZpbGU9IiQxIgogIGxvY2FsIGJha3VwX3N1ZmZpeD0iJChkYXRlIC0tdXRjICsiVklbSVkJUglTSIpIgogIAoKICBpZiBncmVwIC1xICEgLnZcm1hdE1zZ05vTG9va3Vwcz10cnVlJyAkZmlsZQogIHRoZW4gCiAgICBsb2dfbWVzc2FnZV9sb2c0aiAiVGhlIGphdmEgcHJvcGVydHkgbG9nNGoyLmZvcm1hdE1zZ05vTG9va3Vwcz10cnVlIGlzIGFscmVhZHkgc2V0IGluICRmaWxlLiIKICBlbHNlIAogICAgbG9nX2luZm9fbWVzc2FnZV9sb2c0aiAiQ3JlYXRpbmcgYmFjayB1cCBmb3Igc2V0ZW52IGZpbGUgaW4gJGZpbGUuJGJha3VwX3N1ZmZpeCIKICAgIGNwIC1mICIkZmlsZSIgIiRmaWxlLiRiYWt1cF9zdWZmaXgiCiAgICBsb2dfbWVzc2FnZV9sb2c0aa

iAiQWRkaW5nIC1EbG9nNGoyLmZvcm1hdE1zZ05vTG9va3Vwcz10cnVlIHRvIEpWTV9PUFRTIGluICRmaWxlI
gogICAgcmVzPSQoYXdrICdGTll9PU5SeyBpZiAoL15KVk1fT1BUUz0vKSBwPU5SOyBuZXh0fSAxOyBGTll9PXB
7IHByaW50ICJKVk1fT1BUUz1cIiRKVk1fT1BUUyAtRGxvZzRqMi5mb3JtYXRNc2dOb0xvb2t1cHM9dHJ1ZVwiI
iB9JyAkZmlsZSAkZmlsZSkgfHwgbG9nX2Vycm9yX2xvZzRqICJGYWlsZWQgdG8gZWRpdCAkZmlsZSIKICAgIG
VjaG8gIiRyZXMiID4gJGZpbGUKICBmaQp9Cgp1cGRhdGVfdnJvX3RvbWNhdF9zdGFydCgpIHsKICBsb2NhbC
BmaWxlPSIkMSIKCiAgaWYgZ3JlcCAtcSAncGF0Y2hfYWxsX3BsdWdpbnNfdjIgPicgJGZpbGUKICB0aGVuIAog
CAgbG9nX21lc3NhZ2VfbG9nNGogIk5vdGhpbmcgdG8gZG8uIEtCIGFscmVhZHkgYXBwbGllZCEiCiAgZWxzZ
QogICAgbG9jYWwgcmVzCiAgICBsb2NhbCBiYWt1cF9zdWZmaXg9IiQoZGF0ZSAtLXV0YyArIiVZJW0lZCVIJU0
iKSIKICAgIGxvZ19tZXNzYWdlX2xvZzRqICJDcmVhdGluZyBiYWNrIHVwIGZvciB0b21jYXQgc3RhcnR1cCBjb25
maWcgaW4gJGZpbGUuJGJha3VwX3N1ZmZpeCIKICAgIGNwIC1mICIkZmlsZSIgIiRmaWxlLiRiYWt1cF9zdWZ
maXgiCgogICAgbG9nX21lc3NhZ2VfbG9nNGogIk1vZGlmeWluZyB2Uk8gdG9tY2F0IHN0YXJ0dXAgY29uZml
nIC0gJGZpbGUiCgogICAgaWYgZ3JlcCAtcSAnI2xvZzRqX2N2ZV93b3JrYXJvdW5kJyAkZmlsZQogICAgdGhlbgo
gICAgICBzZWQgLWkgJ3MvI2xvZzRqX2N2ZV93b3JrYXJvdW5kL1xuI2xvZzRqX2N2ZV93b3JrYXJvdW5kL2cnI
CRmaWxlCiAgICAgIHNlZCAtaSAnL2xvZ19tZXNzYWdlX2xvZzRqMl9jdmUgIlBhdGNoaW5nIGRvbmUuIiQve2
47cy8uKi99XG4jbG9nNGpfY3ZlX3dvcmthcm91bmRfZW5kL30nICRmaWxlCiAgICAgIHNlZCAtaSAnL3ZSTyBz
ZXJ2ZXIgc2VydmljZSBkaWQgbm90IHN0YXJ0IHdpdGhpbiB0aGUgZXhwZWN0ZWQgcGVyaW9kLiokL3tuO2
47bjtzLy4qL31cbiNsb2c0al9jdmVfd29ya2Fyb3VuZF9lbmQvfScgJGZpbGUKICAgICAgc2VkIC1pICcvI2xvZzRq
X2N2ZV93b3JrYXJvdW5kLywvI2xvZzRqX2N2ZV93b3JrYXJvdW5kX2VuZC9jXGRlbGV0ZV9tYXJrZXJcJyAkZmls
ZQogICAgICBwZXJsIC1pIC0wcGUgJ3MvKC4qKVxuLipkZWxldGVfbWFya2VyXG4vXDEvZzsnICRmaWxlCgogI
CAgICBzZWQgLWkgJy9sb2c0al9jdmVfd29ya2Fyb3VuZCA+L2QnICRmaWxlIAogICAgICBzZWQgLWkgJy9wY
XRjaF9hbGxfcGx1Z2lucyA+L2QnICRmaWxlCiAgICBmaQogICAgICBmaQogICAgICBzZWQgLWkgJy9wYmFzZTY0IC1kIDw8PC9kJyAk
ZmlsZSAKCiAgICBpZiAhIGdyZXAgLXFFICdhY3Rpb249InN0YXJ0InxTdGFydGluZyB0Y1NlcnZlcicgIiRmaWxlIgo
gICAgdGhlbgogICAgICBsb2dfZXJyb3JfbG9nNGogIlVuYWJsZSB0byBhcHBseSBwYXRjaDogVW5leHBlY3RlZC
Bmb3JtYXQgb2YgdlJPIHRvbWNhdCBzdGFydHVwIGNvbmZpZyAtICRmaWxlLiIKICAgICAgZXhpdCAxCiAgICB
maQoKICAgIGxvY2FsIHV0aWw9IiQoZGlybmFtZSAiJGZpbGUiKS9jdmVfdXRpbC5zaCIKICAgIGJhc2U2NCAtZ
CA8PDwgIkkyeHZaelJxWDJOMlpWOTNiM0pyWVhkdmRXNWtDbXh2WjE5dFpYTnpZV2RsWDJ4dlp6UnFN
bDlqZG1WZmRqSW9LU0l3Q2dsbFkyaHZJQ0piSkNoa1lYUmxJQzB0ZFhSakIDSXJKVVpVSlZRdUpUTk9XaUlw
WFNBa01TSUtmUW9LQ25CaGRHTm9YM0JzZFdkcGJsOTJNaWdwSUhzS0NXeHZZMkZzSUhCc2RXZHBibDl3
WVhSb1BTSWtNU0lLQ1d4dlkyRnNJSEJzZFdkcGJsOXVZVzFsUFNJa0tHSmhjMlZ1WVcxbElDSWtjR3gxWjJsd
VgzQmhkR2dpS1NJS0NXeHZZMkZzSUhSbGJYQmZjR0YwYUQwaUwzUnRjQzhrY0d4MVoybHVYMjVoYldVa
UNnbHNiMk5oYkNCaVlXTnJkWEJ6WDNCaGRHZzlJaTkxYzNJdmJHbGlMM1pqYnk5aVlXTnJkWEJ6SWdvS0N
XMXJaR2x5SUMxd0lDSWtZbUZqYTNWd2MxOXdZWFJvSWdvS0NYSnRJQzF5WmlBaUpIUmxiWEJmY0dGM
GFDSUtDWFZ1ZW1sd0lDMXhJQ0lrY0d4MVoybHVYM0JoZEdnaUlDMWtJQ0lrZEdWdGNGOXdZWFJvSWlC
OGZDQmxlR2wwSURFS0Nna2pJRU5vWldOcklHbG1JSFJvWlhKbElHbHpJR0VnYm1WbFpDQjBieUIxY0dSaG
RHVWdkR2hsSUhCc2RXZHBiZ29KYVdZZ1ptbHVaQ0FpSkhSbGJYQmZjR0YwYUNJZ0xYaGtaWFlnTFhSNWNH
VWdaaUF0Ym1GdFpTQW5iRzluTkdvdFkyOXlaUzB5S21waGNpY2dMV1Y0WldNZ0wzVnpjaTlpYVc0dmVtb
HdJQzF6WmlBaWUzMGlJRnc3SUh3Z1ozSmxjQ0J2Y21jdllYQmhZMmhsTDJ4dloyZHBibWN2Ykc5bk5Hb3ZZ
Mjl5WlM5c2IyOXJkWEF2U201a2FVeHZiMnQxY0M1amJHRnpjenNLQ1hSb1pXNEtDUWxzYjJkZmJXVnpjMk
ZuWlY5c2IyYzBhakpmWTNabFgzWXlJQ0pOYjJScFpubHBibWNnY0d4MVoybHVPaUFrY0d4MVoybHVYMjVo
YldVaUNna0piWFlnSWlSd2JIVm5hVzVmY0dGMGFDSWdJaVJpWVdOcmRYQnpYM0JoZEdnaUNna0pabWx
1WkNBaUpIUmxiWEJmY0dGMGFDSWdMWGhrWlhZZ0xYUjVjR1VnWmlBdGJtRnRaU0FuYkc5bk5Hb3RZMj
l5WlMweUttcGhjaWNnTFdWNFpXTWdjMmdnTFdNZ0p5OTFjM0l2WW1sdUwzcHBjQ0F0Y1NBdFpDQWll

MzBpSUc5eVp5OWhjR0ZqYUdVdmJHOW5aMmx1Wnk5c2IyYzBhaTlqYjNKbEwyeHZiMnQxY0M5S2JtUnBU
Rzl2YTNWd0xtTnNZWE56T3lCMGIzVmphQ0F0ZENBeU1ESXhNREV3TVRBd01EQWdJbnQ5SWljZ1hEc0tDU
WtvWTJRZ0lpUjBaVzF3WDNCaGRHZ2lJRHNnZW1sd0lDMXhJQzF5SUMxWUlDMUVJQ0lrY0d4MVoybHVY
M0JoZEdnaUlDb3BJSHg4SUdWNGFYUWdNUW9LQ1FraklFWnBlQ0J5YVdkb2RITUtDUWxqYUc5M2JpQjJZ
Mjg2ZG1OdklDSWtjR3gxWjJsdVgzQmhkR2dpQ2drSlkyaHRiMlFnTURZME5DQWlKSEJzZFdkcGJsOXdZWFJv
SWdvSkNXeHZaMTl0WlhOeIlXZGxYMnh2WnpScU1sOWpkbVZmZGpJZ0lsTjFZMk5sYzNObWRXeHNlU0J3W
VhSamFHVmtJSEJzZFdkcGJqb2dKSEJzZFdkcGJsOXVZVzFsSWdvSlpXeHpaUW9KQ1d4dloxOXRaWE56WVdkb
FgyeHZaelJxTWw5amRtVmZkaklnSWs1dmRHaHBibWNnZEc4Z1pHOGdabTl5SUhCc2RXZHBiam9nSkhCc2R
XZHBibDl1WVcxbElnb0pabWtLQ1hKdElDMXlaaUFpSkhSbGJYQmZjR0YwYUNJS2ZRb0tjR0YwWTJoZllXeHN
YM0JzZFdkcGJuTmZkaklvS1NCN0NnbG1iM0lnWm1sc1pTQnBiaUF2ZFhOeUwyeHBZaTkyWTI4dllYQndMW
E5sY25abGNpOXdiSFZuYVc1ekx5b3VaR0Z5Q2dsa2J3b0pDWEJoZEdOb1gzQnNkV2RwYmw5Mk1pQWlKR1
pwYkdVaUlIeDhJR3h2WjE5dFpYTnpZV2RsWDJ4dlp6UnFNbDlqZG1WZmRqSWdJa1ZTVWs5U09pQkdZV2xz
WldRZ2RHOGdjR0YwWTJnZ2NHeDFaMmx1T2lBa0tHSmhjMlZ1WVcxbElDUm1hV3hsS1NJS0NXUnZibVVLQ
2dsc2IyZGZiV1Z6YzJGblpWOXNiMmMwYWpKZlkzWmxYM1l5SUNKUVlYUmphR2x1WnlCa2IyNWxMaUlLZl
FvPSIgPiAiJHV0aWwiCgogICAgc2VkIC1pICdzLGV2YWwgZXhlYywnInNvdXJjZSAkdXRpbCInXG4mLCcgIiRma
WxlIgogICAgZ3JlcCAtcSAic291cmNlICR1dGlsIiAiJGZpbGUiIHx8IHsgbG9nX2Vycm9yX2xvZzRqICJGYWlsZWQ
gdG8gZWRpdCAkZmlsZS4gQmFja3VwIGNhbiBiZSBmb3VuZCBpbiAkZmlsZS4kYmFrdXBfc3VmZml4IjsgZXhp
dCAxOyB9CgogICAgc2VkIC1yIC1pICcvYWN0aW9uPSJzdGFydCJ8U3RhcnRpbmcgdGNTZXJ2ZXIvYSBcXHRcd
Fx0cGF0Y2hfYWxsX3BsdWdpbnNfdjIgPj4gL3Zhci9sb2cvdm13YXJlL3Zjby9hcHAtc2VydmVyL3Zjb19sb2c0al
9jdmUubG9nJyAkZmlsZQogICAgZ3JlcCAtcSAncGF0Y2hfYWxsX3BsdWdpbnNfdjIgPicgIiRmaWxlIiB8fCB7IGx
vZ19lcnJvcl9sb2c0aiAiRmFpbGVkIHRvIGVkaXQgJGZpbGUuIEJhY2t1cCBjYW4gYmUgZm91bmQgaW4gJGZp
bGUuJGJha3VwX3N1ZmZpeCI7IGV4aXQgMTsgfQoKICAgIGxvZ19tZXNzYWdlX2xvZzRqICJTdWNjZXNzZnVsb
HkgbW9kaWZpZWQgdGhlIHZSTyB0b21jYXQgc3RhcnR1cCBjb25maWcgLSAkZmlsZSIKICBmaQp9CgoKKHNl
dF9qYXZhX29wdCAiL3Vzci9saWIvdmNvL2NvbmZpZ3VyYXRpb24vYmluL3NldGVudi5zaCIgJiYgc2V0X2phdm
Ffb3B0ICIvdXNyL2xpYi92Y28vYXBwLXNlcnZlci9iaW4vc2V0ZW52LnNoIiAmJiB1cGRhdGVfdnJvX3RvbWNhd
F9zdGFydCAiL3Zhci9saWIvdmNvL2FwcC1zZXJ2ZXIvYmluL2luaXQuZC5zaCIpIHx8IGxvZ19lcnJvcl9sb2c0aiAi
RmFpbGVkIHRvIGFwcGx5IHRoZSBsb2c0aiBDVkUgd29ya2Fyb3VuZCBmb3IgdlJPLiBGb3IgbW9yZSBkZXRha
WxzIHNlZSAvdmFyL2xvZy92bXdhcmUvdmNvL2FwcC1zZXJ2ZXIvdmNvX2xvZzRqX2N2ZS5sb2cuIg==" | sh –

4. Ejecutar el siguiente comando en cada nodo para actualizar el “Control Center”:

   /usr/lib/vco/tools/configuration-cli/bin/vro-configure-inner.sh controlcenter-update

5. Reiniciar los servicios en cada nodo:

   service vco-server restart && service vco-configurator start

6. Para validar que el workaround haya sido exitoso seguir los siguientes pasos en cada uno de los nodos:
   a. Verificar que todos los procesos de vco están corriendo con la propiedad **"log4j2.formatMsgNoLookups=true"** con el siguiente comando: *ps aux | grep -i java | grep Dlog4j2.formatMsgNoLookups=true*

b. Revisar el log */var/log/vco/app-server/vco_log4j_cve.log* hasta que se vea 'Patching done.'
c. Correr el siguiente comando para verificar que **JndiLookup.class** no esté presente en ningún archivo de log4j jar para versiones de 2.x. Este no debe devolver ningún output: *find / -xdev -type f -name 'log4j-core-2*jar' -exec sh -c '/usr/bin/unzip -l "{}" | grep org/apache/logging/log4j/core/lookup/JndiLookup.class' \;*

Método de Rollback

- Restaurar los backups

Links de referencia

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

https://kb.vmware.com/s/article/87120

https://kb.vmware.com/s/article/87121

https://kb.vmware.com/s/article/87122