Las Javas se ponen al día aplican los controles CRL por abandono que previene el NSP y al invitado fluye

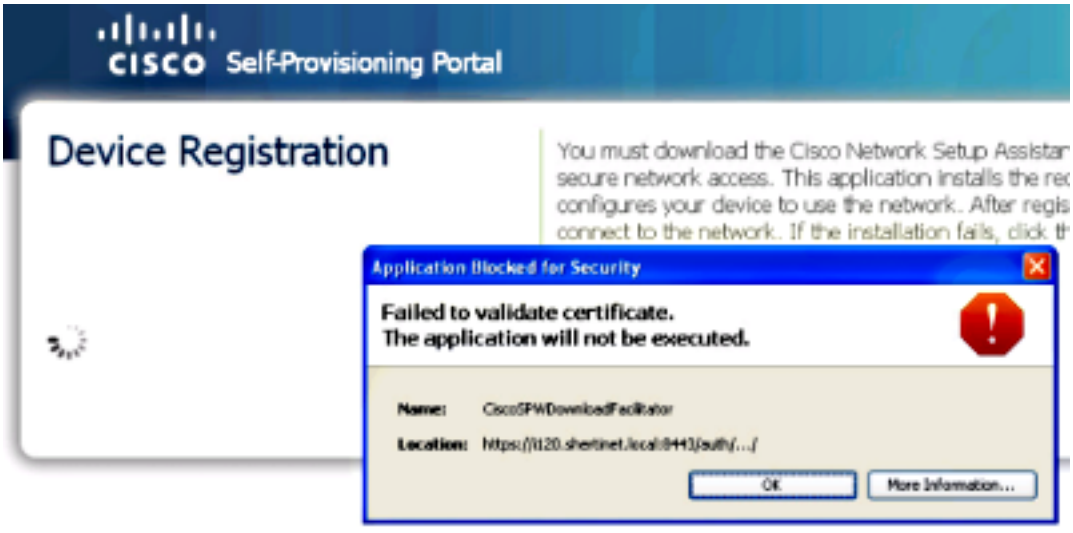
Contenido

Introducción

Este documento describe un problema encontrado donde la última actualización de las Javas rompe la disposición del supplicant y algunos flujos del invitado que utilizan el Listas de control de acceso (ACL) y el cambio de dirección.

Antecedentes

El error está en el CiscoSPWDownloadFacilitator y lee “no podido validar el certificado. La aplicación no será ejecutada.”



Si usted hace clic **más información**, usted recibe la salida que se queja por el Listas de revocación de certificados (CRL).

```
java.security.cert.CertificateException: java.security.cert.
CertPathValidatorException: java.io.IOException: DerInputStream.getLength():
lengthTag=127, too big.
at com.sun.deploy.security.RevocationChecker.checkOCSP(Unknown Source)
at com.sun.deploy.security.RevocationChecker.check(Unknown Source)
at com.sun.deploy.security.TrustDecider.checkRevocationStatus(Unknown Source)
at com.sun.deploy.security.TrustDecider.getValidationState(Unknown Source)
at com.sun.deploy.security.TrustDecider.validateChain(Unknown Source)
at com.sun.deploy.security.TrustDecider.isAllPermissionGranted(Unknown Source)
at sun.plugin2.applet.Plugin2ClassLoader.isTrustedByTrustDecider
(Unknown Source)
at sun.plugin2.applet.Plugin2ClassLoader.getTrustedCodeSources(Unknown Source)
at com.sun.deploy.security.CPCallbackHandler$ParentCallback.strategy
(Unknown Source)
at com.sun.deploy.security.CPCallbackHandler$ParentCallback.openClassPathElement
(Unknown Source)
at com.sun.deploy.security.DeployURLClassPath$JarLoader.getJarFile
(Unknown Source)
at com.sun.deploy.security.DeployURLClassPath$JarLoader.access$1000
(Unknown Source)
at com.sun.deploy.security.DeployURLClassPath$JarLoader$1.run(Unknown Source)
at java.security.AccessController.doPrivileged(Native Method)
at com.sun.deploy.security.DeployURLClassPath$JarLoader.ensureOpen
(Unknown Source)
at com.sun.deploy.security.DeployURLClassPath$JarLoader.<init>(Unknown Source)
at com.sun.deploy.security.DeployURLClassPath$3.run(Unknown Source)
at java.security.AccessController.doPrivileged(Native Method)
at com.sun.deploy.security.DeployURLClassPath.getLoader(Unknown Source)
at com.sun.deploy.security.DeployURLClassPath.getLoader(Unknown Source)
at com.sun.deploy.security.DeployURLClassPath.getResource(Unknown Source)
at sun.plugin2.applet.Plugin2ClassLoader$2.run(Unknown Source)
at java.security.AccessController.doPrivileged(Native Method)
at sun.plugin2.applet.Plugin2ClassLoader.findClassHelper(Unknown Source)
at sun.plugin2.applet.Applet2ClassLoader.findClass(Unknown Source)
at sun.plugin2.applet.Plugin2ClassLoader.loadClass0(Unknown Source)
at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)
at sun.plugin2.applet.Plugin2ClassLoader.loadClass0(Unknown Source)
at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)
at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)
at java.lang.ClassLoader.loadClass(Unknown Source)
at sun.plugin2.applet.Plugin2ClassLoader.loadCode(Unknown Source)
at sun.plugin2.applet.Plugin2Manager.initAppletAdapter(Unknown Source)
at sun.plugin2.applet.Plugin2Manager$AppletExecutionRunnable.run(Unknown Source)
at java.lang.Thread.run(Unknown Source)
Suppressed: com.sun.deploy.security.RevocationChecker$StatusUnknownException
at com.sun.deploy.security.RevocationChecker.checkCRLs(Unknown Source)
... 34 more
Caused by: java.security.cert.CertPathValidatorException:
java.io.IOException: DerInputStream.getLength(): lengthTag=127, too big.
at sun.security.provider.certpath.OCSP.check(Unknown Source)
at sun.security.provider.certpath.OCSP.check(Unknown Source)
at sun.security.provider.certpath.OCSP.check(Unknown Source)
... 35 more
Caused by: java.io.IOException: DerInputStream.getLength(): lengthTag=127, too big.
at sun.security.util.DerInputStream.getLength(Unknown Source)
at sun.security.util.DerValue.init(Unknown Source)
at sun.security.util.DerValue.<init>(Unknown Source)
at sun.security.provider.certpath.OCSPResponse.<init>(Unknown Source)
... 38 more
```

Problema

En la última versión de Java (la versión 7, pone al día 25 - 5 de agosto liberado, 2013), el Oracle introdujo una nueva configuración predeterminada que fuerza al cliente a validar el certificado asociado a cualquier applet contra cualquier CRL o protocolo status en línea del certificado (OCSP).

Los socios de firma de Cisco del certificado con estos applet tienen un CRL y un OCSP mencionados con Thawte. Debido a este nuevo cambio, cuando el cliente de las Javas intenta alcanzar hacia fuera a Thawte, es bloqueado por o un puerto ACL y/o una reorientación ACL.

El problema se sigue bajo el Id. de bug Cisco CSCui46739.

Solución

Arreglo del lado del regulador del 1 Switch o de la Tecnología inalámbrica de la opción

1. Reescriba ningunos reorientan o el acceso basado ACL para permitir el tráfico a Thawte y a Verisign. Desafortunadamente, una limitación con esta opción es que los ACL no se pueden crear de los Domain Name.
2. Resuelva la lista CRL manualmente, y póngala en la reorientación ACL.

   Nota: Las reglas de firewall pudieron necesitar ser puesto al día si el cliente necesita comunicar con un Firewall.

```
[user@user-linux logs]$ nslookup
>crl.thawte.com
Server:         64.102.6.247
Address:        64.102.6.247#53

Non-authoritative answer:
crl.thawte.com  canonical name = crl.ws.symantec.com.edgekey.net.
crl.ws.symantec.com.edgekey.net canonical name = e6845.ce.akamaiedge.net.
Name:   e6845.ce.akamaiedge.net
Address: 23.5.245.163

>ocsp.thawte.com
Server:         64.102.6.247
Address:        64.102.6.247#53

Non-authoritative answer:
ocsp.thawte.com canonical name = ocsp.verisign.net.
Name:   ocsp.verisign.net
Address: 199.7.48.72
```

Si el cambio y los clientes de estos nombres DNS resuelven el algo más, reescriba la reorientación URL con los direccionamientos actualizados.

El ejemplo reorienta el ACL:

```
     5 remark ISE IP address
10 deny ip any host X.X.X.X (467 matches)
15 remark crl.thawte.com
   20 deny ip any host 23.5.245.163 (22 matches)
25 remark ocsp.thawte.com
```

```
30 deny ip any host 199.7.52.72
40 deny udp any any eq domain (10 matches)
50 permit tcp any any eq www (92 matches)
60 permit tcp any any eq 443 (58 matches)
```

La prueba ha mostrado la resolución OSCP y CRL URL a estos IP Addresses:

OCSP
199.7.48.72
199.7.51.72
199.7.52.72
199.7.55.72
199.7.54.72
199.7.57.72
199.7.59.72

CRL
23.4.53.163
23.5.245.163
23.13.165.163
23.60.133.163
23.61.69.163
23.61.181.163

Esto no pudo ser una lista completa y pudo cambiar basado en la geografía, así que la prueba se requiere para descubrir qué direcciones IP resuelven los host en a cada caso.

Opción 2 - Arreglo del lado del cliente

Dentro de la sección **avanzada del** panel de control Java, el conjunto **realiza los controles de la revocación de certificado encendido no marca (no recomendado)**.

OSX: **Preferencias > Javas del sistema**
Avanzado
Realice la revocación de certificado usando: El cambio “no marca (no recomendado)”

Windows: **Panel de control > Javas**
Avanzado
Realice la revocación de certificado usando: El cambio “no marca (no recomendado)”