Java Update voert standaard CRL-controles in waardoor NSP- en Guest-stromen worden voorkomen

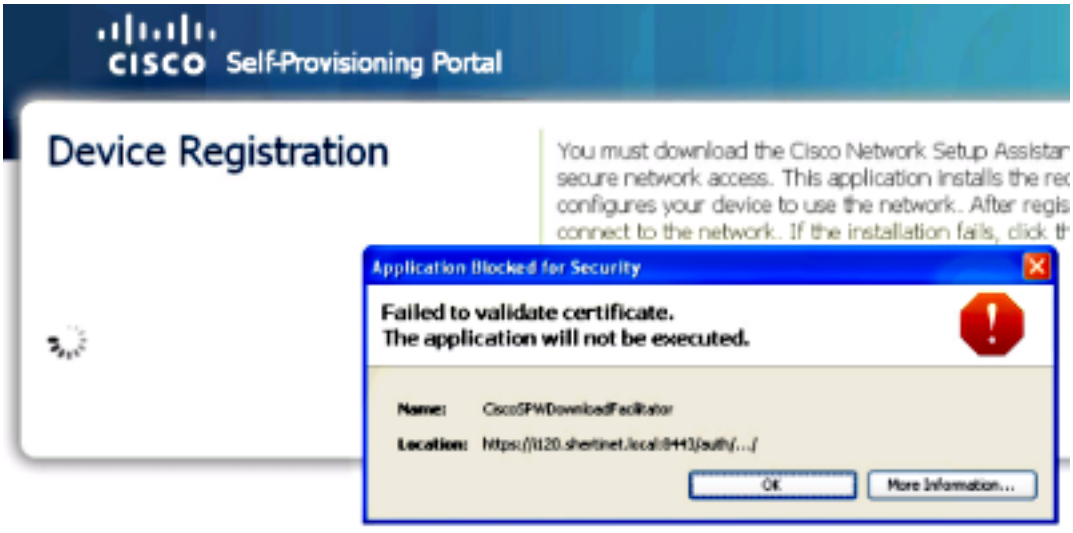
Inhoud

Inleiding

Dit document beschrijft een ondervonden probleem waar de nieuwste Java-update leveringsonderbrekingen en sommige gaststromen die toegangscontrolelijsten (ACL's) en omleiding gebruiken.

Achtergrondinformatie

De fout staat in de Cisco SPWDownloadFacilitator en luidt "Is mislukt om certificaat te valideren. De applicatie zal niet worden uitgevoerd."



Als u op **Meer informatie** klikt, ontvangt u uitvoer die klacht indient over de lijst certificaatherroeping (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
```

Probleem

In de meest recente versie van Java (Versie 7, Update 25 - uitgebracht op 5 augustus 2013) introduceerde Oracle een nieuwe standaardinstelling die de client dwingt om het certificaat te valideren dat aan een toepassing is gekoppeld, tegen een CRL- of Online certificaatprotocol (OCSP).

Het ondertekeningscertificaat dat Cisco geassocieerd is met deze applets heeft een lijst CRL en OCSP met Thawte. Vanwege deze nieuwe wijziging, wanneer de Java-client probeert om Thawte te bereiken, wordt het geblokkeerd door een poort-ACL en/of opnieuw-ACL.

Het probleem wordt getraceerd onder Cisco bug-ID CSCui46739.

Oplossing

Optie 1 - Switch of draadloze controller op Side Fix

1. Herschrijft om het even welke herleiding of op poort gebaseerde ACLs om verkeer naar Thawte en Versizing toe te staan. Helaas is één beperking met deze optie dat ACL's niet van domeinnamen kunnen worden gemaakt.
2. Los de CRL lijst handmatig op en plaats het in de herleiding ACL.

   Opmerking: Firewallregels moeten misschien worden bijgewerkt als de client door een firewall moet communiceren.

```
[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
```

Als deze DNS namen veranderen en de klanten iets anders oplossen, herschrijf de URL met de bijgewerkte adressen.

Voorbeeld omleiden 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)
```

Bij het testen is de vastberadenheid van OSCP en CRL URL's op deze IP-adressen weergegeven:

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

Dit zou geen volledige lijst kunnen zijn en zou kunnen veranderen gebaseerd op geografie, dus het testen is vereist om te ontdekken welk IP adres(en) de hosts in elk geval tot stand brengt.

Optie 2 - Clientzijfilter

In het **geavanceerde** gedeelte van het Java Control Panel **voert u** de **herroepingscontroles van certificaten uit** om deze **niet te controleren (niet aanbevolen)**.

OSX: **Systeemvoorkeuren > Java**
Geavanceerd
Herroeping van certificaat uitvoeren met behulp van: Wijzigen naar 'Niet controleren (niet aanbevolen)'

Windows: **Bedieningspaneel > Java**
Geavanceerd
Herroeping van certificaat uitvoeren met behulp van: Wijzigen naar 'Niet controleren (niet aanbevolen)'