Javas mettent à jour imposent des contrôles CRL par défaut qui empêche le NSP et l'invité circule

Contenu

Introduction

Ce document décrit un problème rencontré où la dernière mise à jour de Javas casse le ravitaillement de suppliant et quelques écoulements d'invité qui utilisent le Listes de contrôle d'accès (ACL) et la redirection.

Informations générales

L'erreur est dans le CiscoSPWDownloadFacilitator et lit « pour valider le certificat. L'application ne sera pas exécutée. »

Si vous cliquez sur **plus d'informations**, vous recevez la sortie qui se plaint au sujet du Liste des révocations de certificat (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
```

Problème

Dans la dernière version de Javas (version 7, mise à jour 25 - 5 août libéré, 2013), Oracle a introduit une nouvelle valeur par défaut qui force le client pour valider le certificat associé avec n'importe quel applet contre n'importe quel CRL ou état en ligne Protocol (OCSP) de certificat.

Les associés de signature de Cisco de certificat avec ces applet a un CRL et un OCSP énumérés avec Thawte. En raison de cette nouvelle modification, quand les tentatives de client java d'atteindre à Thawte, il est bloquées par ou un ACL de port et/ou un ACL de réorientation.

Le problème est dépisté sous l'ID de bogue Cisco CSCui46739.

Solution

Option 1 - Difficulté de côté de commutateur ou de contrôleur sans-fil

1. En réécrivez réorientent ou ACLs basé sur port afin de permettre le trafic à Thawte et à Verisign. Malheureusement, une limite avec cette option est qu'ACLs ne peut pas être créé des noms de domaine.
2. Résolvez la liste CRL manuellement, et mettez-la dans l'ACL de réorientation.

   Remarque: Des règles de Pare-feu pourraient devoir être mises à jour si le client doit communiquer par un Pare-feu.

```
[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 la modification et les clients de ces noms DNS résolvent autre chose, réécrivez l'URL de réorientation avec les adresses mises à jour.

L'exemple réorientent l'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)
```

Le test a affiché la résolution OSCP et CRL URLs à ces adresses IP :

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

Ceci ne pourrait pas être une liste complète et pourrait changer basé sur la zone géographique, ainsi le test est exigé pour découvrir quelles adresses IP les hôtes résolvent à dans chaque exemple.

Option 2 - Difficulté de côté client

Àl'intérieur de la section **avancée du** panneau de contrôle Java, le positionnement **exécutent des contrôles de révocation de certificat en fonction ne vérifient pas (non recommandé)**.

OSX : **Préférences Système > Javas**
Avancé
Effectuez la révocation de certificat utilisant : La modification « ne vérifient pas (non recommandé) »

Windows : **Panneau de configuration > Javas**
Avancé
Effectuez la révocation de certificat utilisant : La modification « ne vérifient pas (non recommandé) »