As Javas atualizam reforçam verificações CRL à revelia que impedem o NSP e o convidado fluem

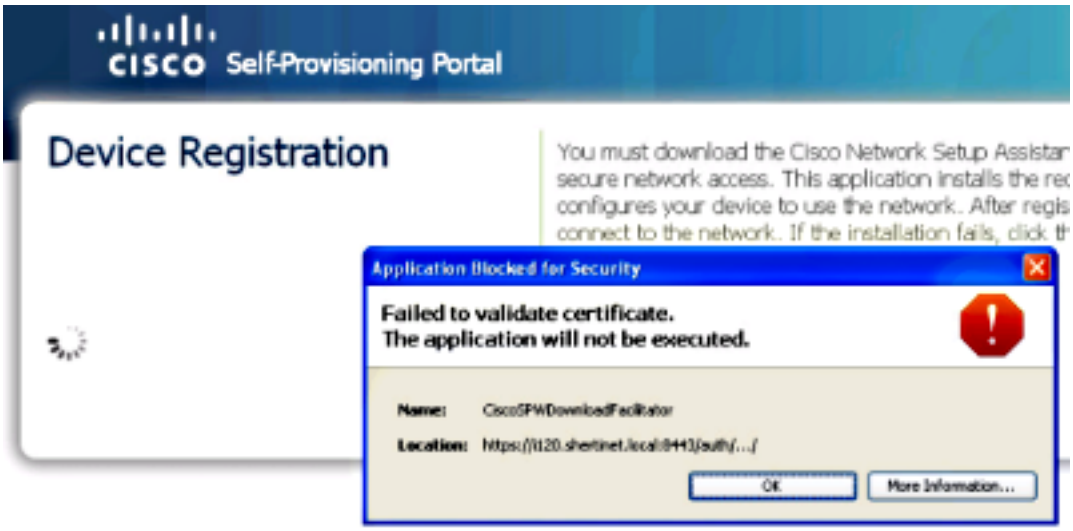
Índice

Introdução

Este documento descreve um problema encontrado onde a atualização a mais atrasada das Javas quebra o abastecimento do suplicante e os alguns fluxos do convidado que usam o Access Control Lists (ACLs) e a reorientação.

Informações de Apoio

O erro está no CiscoSPWDownloadFacilitator e lê “não valida o certificado. O aplicativo não será executado.”



Se você clica **mais informação**, você recebe a saída que se queixa sobre o Certificate Revocation List (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

Na versão de java a mais atrasada (a versão 7, atualiza 25 - o 5 de agosto liberado, 2013), o Oracle introduziu uma configuração padrão nova que forçasse o cliente a validar o certificado

associado com todo o applet contra qualquer CRL ou protocolo status em linha do certificado (OCSP).

Os associados de assinatura de Cisco do certificado com estes applet têm um CRL e um OCSP listados com Thawte. Devido a esta mudança nova, quando o cliente das Javas tenta alcançar para fora a Thawte, é obstruído ou por uma porta ACL e/ou por uma reorientação ACL.

O problema é seguido sob a identificação de bug Cisco CSCui46739.

Solução

Reparo do lado do controlador do 1 Switch ou do Sem fio da opção

1. Reescreva alguns reorientam ou ACL com base na porta a fim permitir o tráfego a Thawte e a Verisign. Infelizmente, uma limitação com esta opção é que os ACL não podem ser criados dos Domain Name.
2. Resolva a lista CRL manualmente, e põe-na na reorientação ACL.

   Nota: As regras do Firewall puderam precisar de ser atualizado se o cliente precisa de se comunicar com um 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
```

Se a mudança e os clientes destes nomes de DNS resolvem algo mais, reescreva a reorientação URL com os endereços actualizados.

O exemplo reorienta o 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)
```

Os testes mostraram a resolução OSCP e CRL URL a estes endereços IP de Um ou Mais Servidores Cisco ICM NT:

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

Esta não pôde ser uma lista completa e pôde mudar baseado na geografia, assim que os testes são exigidos para descobrir que endereços IP de Um ou Mais Servidores Cisco ICM NT os anfitriões resolvem em cada exemplo.

Opção 2 - Reparo do lado do cliente

Dentro da seção **avançada do** painel de controle de Java, o grupo **executa verificações da revogação de certificado sobre não verifica (não recomendado)**.

OSX: **Preferências > Javas do sistema**
Avançado
Execute a utilização da revogação de certificado: A mudança “não verifica (não recomendado)”

Windows: **Control Panel > Javas**
Avançado
Execute a utilização da revogação de certificado: A mudança “não verifica (não recomendado)”