Java Update setzt standardmäßig CRL-Prüfungen durch, wodurch NSP und Gastflüsse verhindert werden.

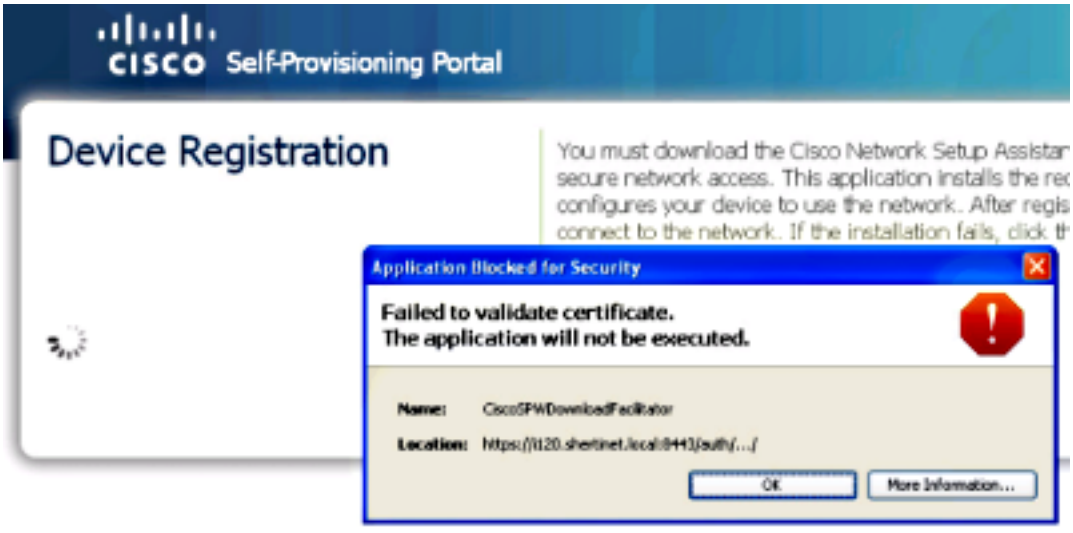
Inhalt

Einführung

In diesem Dokument wird ein Problem beschrieben, bei dem bei der neuesten Java-Aktualisierung die Komponentenbereitstellung sowie einige Gastdatenflüsse, die Zugriffskontrolllisten (ACLs) und Umleitungen verwenden, unterbrochen werden.

Hintergrundinformationen

Der Fehler befindet sich im CiscoSPWDownloadFacilitator und lautet "Fehler bei der Validierung des Zertifikats. Die Anwendung wird nicht ausgeführt."



Wenn Sie auf **Weitere Informationen** klicken, erhalten Sie eine Ausgabe, die sich über die CRL (Certificate Revocation List) beschwert.

```
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
```

Problem

In der neuesten Java-Version (Version 7, Update 25 - veröffentlicht am 5. August 2013) hat Oracle eine neue Standardeinstellung eingeführt, die den Client zwingt, das mit einem Applet verknüpfte Zertifikat gegen ein CRL- oder Online Certificate Status Protocol (OCSP) zu validieren.

Das Signaturzertifikat, das Cisco diesen Applets zuordnet, enthält ein aufgeführtes CRL und ein aufgeführtes OCSP mit Thawte. Wenn der Java-Client versucht, Thawte zu erreichen, wird er aufgrund dieser neuen Änderung entweder durch eine Port-ACL und/oder eine Umleitungs-ACL blockiert.

Das Problem wird unter der Cisco Bug-ID CSCui46739 nachverfolgt.

Lösung

Option 1: Fehlerbehebung auf der Seite des Switches oder Wireless Controllers

1. Umschreiben von Umleitungen oder portbasierten ACLs, um Datenverkehr zu Thawte und Verisign zuzulassen. Leider besteht eine Einschränkung bei dieser Option darin, dass ACLs nicht aus Domänennamen erstellt werden können.
2. Nehmen Sie die CRL-Liste manuell auf, und legen Sie sie in die umgeleitete ACL ein.

   Hinweis: Firewall-Regeln müssen möglicherweise aktualisiert werden, wenn der Client über eine Firewall kommunizieren muss.

```
[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
```

Wenn sich diese DNS-Namen ändern und Clients etwas Anderes auflösen, schreiben Sie die Umleitungs-URL mit den aktualisierten Adressen um.

Beispiel für Umleitungszugriffskontrollliste:

```
     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)
```

Die Tests haben gezeigt, dass die OSCP- und CRL-URLs zu diesen IP-Adressen aufgelöst werden:

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

Dies ist möglicherweise keine vollständige Liste und kann sich je nach Region ändern. Daher sind Tests erforderlich, um zu ermitteln, auf welche IP-Adresse(n) die Hosts in jeder Instanz auflösen.

Option 2 - Client-seitige Programmkorrektur

Legen Sie im **erweiterten** Bereich des Java-Systemsteuerungsfensters fest, dass die Option **Zertifikat-Widerruf** ausführen auf **Nicht aktivieren (nicht empfohlen)** aktiviert **ist**.

OSX: **Systemeinstellungen > Java**
Erweitert
Zertifikat-Widerruf durchführen mit: Ändern Sie die Einstellung in "Nicht überprüfen (nicht empfohlen)".

Windows: **Systemsteuerung > Java**
Erweitert
Zertifikat-Widerruf durchführen mit: Ändern Sie die Einstellung in "Nicht überprüfen (nicht empfohlen)".