تفرض خدمة تحديث Java عمليات التحقق من قائمة التحكم في الوصول (CRL) بشكل افتراضي والتي تمنع تدفق NSP والضيف

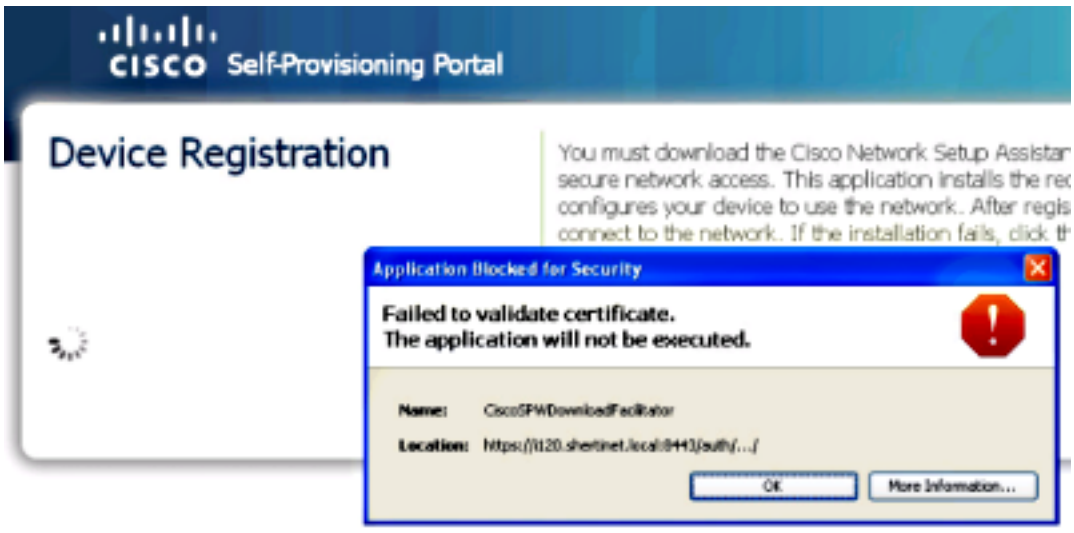
المحتويات

المقدمة

يصف هذا المستند مشكلة تمت مصادفتها حيث يكسر أحدث تحديث Java إعداد الطلب وبعض تدفقات الضيوف التي تستخدم قوائم التحكم في الوصول (ACLs) وإعادة التوجيه.

معلومات أساسية

يوجد الخطأ في CiscoSPWDownloadFacilitator ويقرأ "فشل في التحقق من صحة الشهادة. لن يتم تنفيذ التطبيق.



إذا نقرت فوق **مزيد من المعلومات**، فستتلقى مخرجات تشكو من قائمة إلغاء الشهادة (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
                                                            more 34 ...
                       :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
                                                            more 35 ...
.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
                                                            more 38 ...
```

المشكلة

في أحدث إصدار من Java (الإصدار 7، Update 25 - تم إصداره في 5 أغسطس 2013)، قامت Oracle بإدخال

إعداد افتراضي جديد يفرض على العميل التحقق من صحة الشهادة المرتبطة بأي برنامج صغير مقابل أي بروتوكول حالة الشهادة عبر الإنترنت (CRL) أو بروتوكول حالة الشهادة عبر الإنترنت (OCSP).

تحتوي شهادة التوقيع التي تقترن بها Cisco مع هذه التطبيقات على CRL و OCSP مسرودين مع Thawte. بسبب هذا التغيير الجديد، عندما يحاول عميل Java الوصول إلى Thawte، يتم حظره إما بواسطة قائمة التحكم في الوصول (ACL) للمنفذ و/أو قائمة التحكم في الوصول (ACL) المعاد توجيهها.

يتم تعقب المشكلة تحت معرف تصحيح الأخطاء من Cisco CSCui46739.

الحل

الخيار 1 - إصلاح جانب المحول أو وحدة التحكم اللاسلكية

1. أعد كتابة أي قوائم تحكم في الوصول (ACL) مستندة إلى المنافذ أو معاد توجيهها للسماح لحركة المرور بالتحويل والإصدار. لسوء الحظ، يوجد قيد واحد مع هذا الخيار وهو أنه لا يمكن إنشاء قوائم التحكم في الوصول من أسماء المجالات.
2. قم بحل قائمة CRL يدويا، ووضعها في قائمة التحكم في الوصول (ACL) المعاد توجيهها.

ملاحظة: قد يلزم تحديث قواعد جدار الحماية إذا كان العميل بحاجة إلى الاتصال من خلال جدار حماية.

```
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
```

إذا تغيرت أسماء DNS هذه وحل العملاء شيئا آخر، أعد كتابة عنوان URL لإعادة التوجيه باستخدام العناوين المحدثة.

مثال على قائمة التحكم في الوصول (ACL) المعاد توجيهها:

```
remark ISE IP address 5
(deny ip any host X.X.X.X (467 matches 10
remark crl.thawte.com 15
(deny ip any host 23.5.245.163 (22 matches 20
remark ocsp.thawte.com 25
deny ip any host 199.7.52.72 30
(deny udp any any eq domain (10 matches 40
(permit tcp any any eq www (92 matches 50
(permit tcp any any eq 443 (58 matches 60
```

أظهر الاختبار حل عناوين IP التالية لعناوين OSCP و CRL:

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

قد لا تكون هذه قائمة كاملة وقد تتغير استنادا إلى الجغرافيا، لذلك يلزم إجراء الاختبار لاكتشاف عنوان (عناوين) IP التي تحل إليها الأجهزة المضيفة في كل مثيل.

الخيار 2 - إصلاح جانب العميل

داخل قسم **المتقدم** من لوحة تحكم جافا، اضبط **تنفيذ تدقيق إبطال الشهادة** على **عدم التحقق (غير مستحسن)**.

OSX: **تفضيلات النظام > Java**
متقدم
إجراء إبطال الشهادة باستخدام: تغيير إلى 'عدم التحقق (غير مستحسن)'

Windows: **لوحة التحكم > Java**
متقدم
إجراء إبطال الشهادة باستخدام: تغيير إلى 'عدم التحقق (غير مستحسن)'

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).