NSP と ゲスト フローを妨げるデフォルトの Java アップデートによる CRL チェックの実施

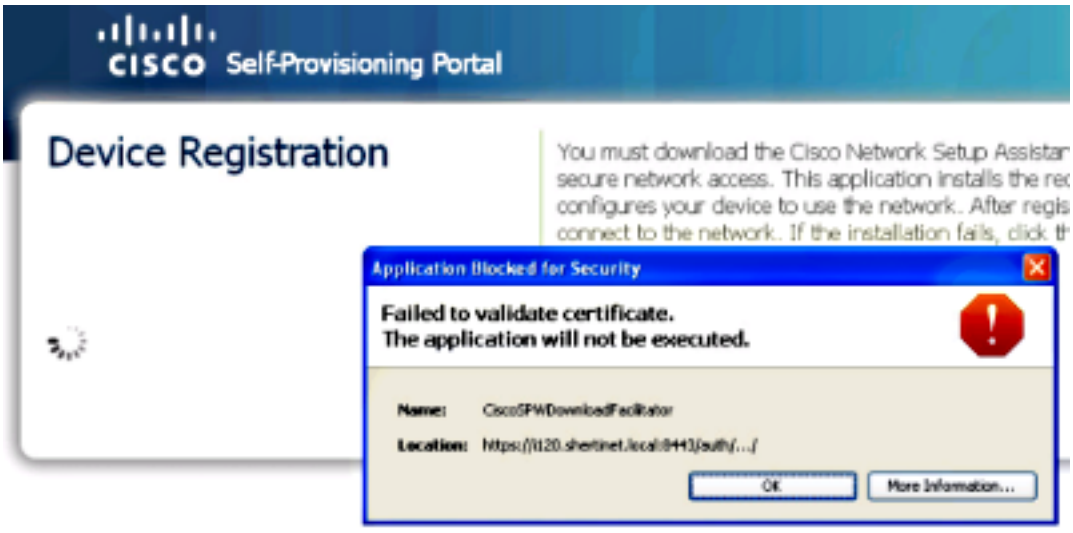
目次

概要

このドキュメントでは、最新の Java アップデートが原因で、アクセス コントロール リスト（ACL）およびリダイレクションを使用する一部のゲスト フローとサプリカント プロビジョニングが中断される問題について説明します。

背景説明

このエラーは CiscoSPWDownloadFacilitator で発生し、「Failed to validate certificate. The application will not be executed.」と出力されます。



[More Information] をクリックすると、証明書失効リスト（CRL）に関するエラーが記述された出力が表示されます。

```
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
```

問題

Oracle は最新バージョンの Java (バージョン 7、 25 - 2013 年 8 月 5 日に公開) で、クライアントがすべてのアプレットに関連付けられている証明書を CRL またはオンライン証明書ステータス

プロトコル（OCSP）と突き合わせて検証するようにする、新しいデフォルト設定を導入しました。

シスコによりこれらのアプレットに関連付けられている署名証明書には、Thawte の CRL と OCSP がリストされています。 この新しい変更に伴い、Java クライアントが Thawte に到達しようとすると、ポート ACL またはリダイレクト ACL のいずれかによりブロックされます。

この問題は Cisco Bug ID CSCui46739 で追跡されます。

解決策

オプション 1 - スイッチまたはワイヤレス コントローラ側の修正

1. Thawte と Verisign へのトラフィックを許可するために、リダイレクト ACL またはポートベースの ACL を編集します。 ただしこの方法では、ACL をドメイン名から作成できないという制約があります。
2. CRL リストを手動で解決し、リダイレクト ACL に追加します。

   注: クライアントがファイアウォール経由で通信する必要がある場合、ファイアウォール ルールを更新する必要があることがあります。

```
[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
```

これらの DNS 名が変更されており、クライアントが他の値を解決した場合は、更新後のアドレスを使用してリダイレクト URL を編集してください。

リダイレクト ACL の例：

```
     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)
```

テストから、OSCP と CRL の URL が次の IP アドレスに解決されることが判明しています。

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

これは完全なリストではなく、地域によって異なる可能性があります。このため、ホストが各インスタンスで解決する IP アドレスをテストで検出する必要があります。

オプション 2 - クライアント側の修正

Java Control Panel の [Advanced] セクション内で、[Perform certificate revocation checks on] を [Do not check (not recommended)] に設定します。

OSX： **[System Preferences] > [Java]**
詳細
次を使用して証明書失効を実行します： [Do not check (not recommended)] に変更します。

Windows： [Control Panel] > [Java]
詳細
次を使用して証明書失効を実行します： [Do not check (not recommended)] に変更します。