Java Update는 NSP 및 게스트 플로우를 방지하는 CRL 검사를 기본적으로 시행합니다.

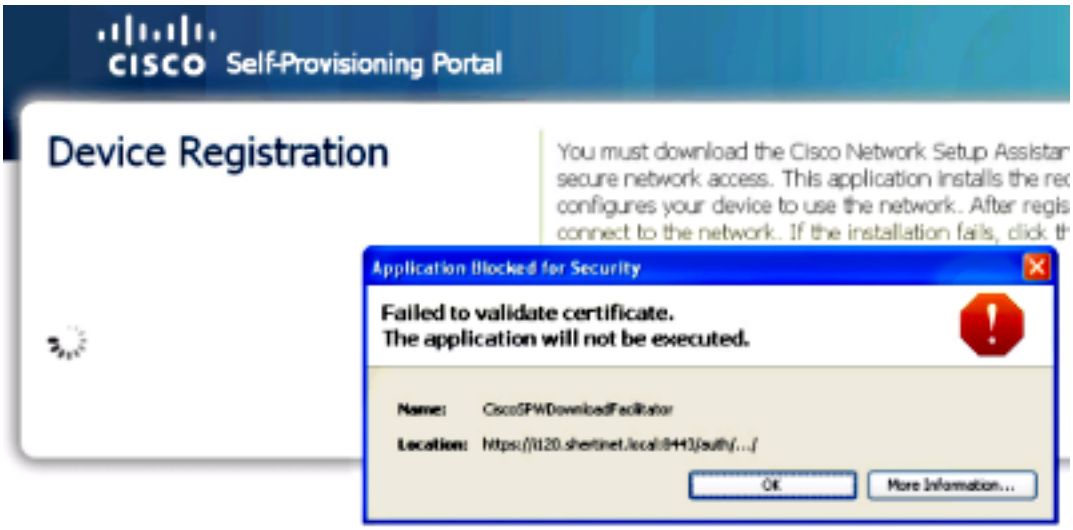
목차

소개

이 문서에서는 최신 Java 업데이트가 서 플리 컨 트 프로비저닝 및 ACL(Access Control Lists) 및 리디렉션을 사용하는 일부 게스트 플로우를 차단하는 문제에 대해 설명합니다.

배경 정보

오류가 CiscoSPWDownload진행자에 있으며 "인증서를 검증하지 못했습니다.응용 프로그램이 실행되지 않습니다."



More Information(**추가 정보)을** 클릭하면 CRL(Certificate Revocation List)에 대해 불평하는 출력이 표시됩니다.

```
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
```

문제

최신 버전의 Java(버전 7, Update 25 - 2013년 8월 5일 릴리스)에서 Oracle은 CRL 또는 OCSP(Online Certificate Status Protocol)에 대해 애플릿과 연관된 인증서를 검증하도록 강제하는

새로운 기본 설정을 도입했습니다.

Cisco가 이러한 애플릿과 연결하는 서명 인증서에는 CRL과 OCSP가 Thawte에 나열되어 있습니다 .이 새로운 변경 사항으로 인해 Java 클라이언트가 Thawte에 연결하려고 시도할 때 포트 ACL 및/또는 리디렉션 ACL에 의해 차단됩니다.

이 문제는 Cisco 버그 ID CSCui46739에서 추적됩니다.

솔루션

옵션 1 - 스위치 또는 무선 컨트롤러 측면 수정

1. 트래픽이 Thawte 및 Verisign으로 이동하도록 모든 리디렉션 또는 포트 기반 ACL을 재작성합니다.안타깝게도 이 옵션의 한 가지 제한 사항은 도메인 이름에서 ACL을 생성할 수 없다는 것입니다.
2. CRL 목록을 수동으로 확인하고 리디렉션 ACL에 넣습니다.

   참고:클라이언트가 방화벽을 통해 통신해야 하는 경우 방화벽 규칙을 업데이트해야 할 수 있습니다.

```
[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
```

이러한 DNS 이름이 변경되고 클라이언트가 다른 문제를 해결할 경우 업데이트된 주소로 리디렉션 URL을 다시 작성하십시오.

리디렉션 ACL 예:

```
     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)
```

테스트에서는 다음 IP 주소로 OSCP 및 CRL URL을 확인합니다.

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

전체 목록이 아닐 수 있으며 지역에 따라 변경될 수 있으므로 각 인스턴스에서 호스트가 확인하는 IP 주소를 검색하려면 테스트가 필요합니다.

옵션 2 - 클라이언트 측 수정

Java 제어판의 **Advanced(고급)** 섹션에서 **Perform certificate revocation checks on(인증서 해지 검사 수행)**을 Do **not check(not recommended)로 설정합니다**.

OSX:**시스템 환경 설정 > Java**
고급
다음을 사용하여 인증서 해지 수행: 'Do not check (not recommended)'로 변경

창:**제어판 > Java**
고급
다음을 사용하여 인증서 해지 수행: 'Do not check (not recommended)'로 변경