默认情况下防止NSP和访客流的Java更新强制执行CRL检查

目录

简介

本文描述遇到的问题最新的Java更新中断使用访问控制列表(ACL)和重定向的请求方设置和一些访客流的地方。

背景信息

错误在CiscoSPWDownloadFacilitator并且读“失败验证证书。应用程序不会被执行”。

如果点击**更多信息**，您收到抱怨证书撤销列表(CRL)的输出。

```
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
```

问题

在Java新版本(版本7，更新25 -发布的8月5， 2013)， Oracle介绍迫使客户端验证证书关联与所有applet任何CRL或联机证书状态协议的一个新的默认设置(OCSP)。

有这些applet的签署的证书思科关联有列出的CRL和OCSP与Thawte。因此新建的更改，当Java客户端尝试提供援助到Thawte时，它由或者端口ACL和重定向ACL阻塞。

问题被跟踪在Cisco Bug ID CSCui46739下。

解决方案

选项1 -交换机或无线控制器旁拉修正

1. 重写所有重定向或基于端口的ACL为了允许流量到Thawte和Verisign。Unforunately，与此选项的一个限制是ACL不可能从域名创建。
2. 手工解决CRL列表，并且放置它在重定向ACL。

注意：如果客户端需要通过防火墙，通信防火墙规则也许需要更新。

```
[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
```

如果这些DNS名名称更改和客户端解决其他，请重写与更新地址的重定向URL。

示例重定向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)
```

测试显示OSCP和CRL URL解决对这些IP地址：

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

这也许不是完整列表，并且也许更改基于地理，因此测试要求发现什么IP地址主机解决对在每个实例。

选项2 -客户端修正

在Java控制面板的**Advanced部分里面，集执行认证吊销检查不检查(不建议使用)**。

OSX ：**系统首选> Java**
先进
执行认证吊销使用： 崔凡吉莱‘不检查(不建议使用)’

Windows ：**控制面板> Java**
先进
执行认证吊销使用： 崔凡吉莱‘不检查(不建议使用)’