Aggiornamento Java applica i controlli CRL per impostazione predefinita impedendo i flussi NSP e Guest

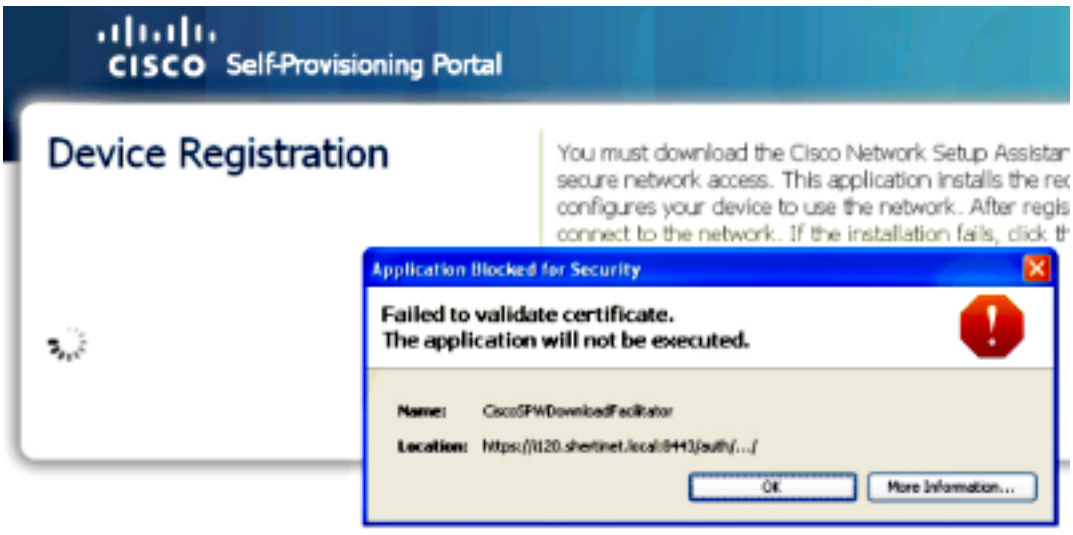
Sommario

Introduzione

In questo documento viene descritto un problema riscontrato quando l'ultimo aggiornamento Java interrompe il provisioning dei supplicant e alcuni flussi guest che utilizzano Access Control Lists (ACL) e il reindirizzamento.

Premesse

L'errore si trova in CiscoSPWDownloadFacilitator e si legge "Impossibile convalidare il certificato. L'applicazione non verrà eseguita."



Se si fa clic su **Ulteriori informazioni**, viene visualizzato un output in cui sono presenti errori relativi all'elenco di revoche di certificati (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)
... 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
```

Problema

Nell'ultima versione di Java (versione 7, aggiornamento 25 - rilasciata il 5 agosto 2013), Oracle ha introdotto una nuova impostazione predefinita che forza il client a convalidare il certificato associato a qualsiasi applet in base a qualsiasi CRL o protocollo di stato del certificato online (OCSP).

Il certificato di firma che Cisco associa a queste applet dispone di un CRL elencato e di un OCSP con Thawte. A causa di questa nuova modifica, quando il client Java tenta di raggiungere Thawte, viene bloccato da un ACL della porta e/o da un ACL di reindirizzamento.

Il problema è segnalato con l'ID bug Cisco CSCui46739.

Soluzione

Opzione 1 - Correzione laterale switch o controller wireless

1. Riscrivere gli ACL di reindirizzamento o basati sulle porte per autorizzare il traffico verso Thawte e Verisign. Sfortunatamente, una delle limitazioni di questa opzione è che gli ACL non possono essere creati da nomi di dominio.
2. Risolvere l'elenco CRL manualmente e inserirlo nell'ACL di reindirizzamento.

   Nota: Potrebbe essere necessario aggiornare le regole del firewall se il client deve comunicare attraverso un firewall.

```
[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
```

Se questi nomi DNS cambiano e i client risolvono qualcos'altro, riscrivere l'URL di reindirizzamento con gli indirizzi aggiornati.

ACL di reindirizzamento di esempio:

```
     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)
```

Il test ha mostrato che gli URL di OSCP e CRL vengono risolti in questi indirizzi IP:

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

Poiché l'elenco potrebbe non essere completo e variare in base all'area geografica, è necessario eseguire un test per individuare gli indirizzi IP a cui gli host eseguono la risoluzione in ogni istanza.

Opzione 2 - Correzione lato client

All'interno della sezione **Advanced** del Pannello di controllo Java, impostare **Perform certificate revocation check on** su **Do not check (scelta non consigliata)**.

OSX: **Preferenze di sistema > Java**
Avanzate
Eseguire la revoca dei certificati utilizzando: Cambia in 'Non selezionare (scelta non consigliata)'

Windows: **Pannello di controllo > Java**
Avanzate
Eseguire la revoca dei certificati utilizzando: Cambia in 'Non selezionare (scelta non consigliata)'