Beheben von Fehlern bei der IOS XE-Zertifikatsvalidierung aufgrund von CDP-URL-Diskrepanzen mit der URL für mehrere CRL-Downloads

Inhalt

Problem

Nachdem einem DMVPN-Hub (Dynamic Multipoint VPN) weitere URL-Adressen für den CRL-Download hinzugefügt wurden, können einige Spoke-Tunnel aufgrund eines Fehlers bei der IKE-Aushandlung nicht eingerichtet werden, und der Hub protokollierte diesen Fehler:

```
%PKI-3-CERTIFICATE_INVALID: Certificate chain validation has failed
```

Die Zertifikatkettenvalidierung ist erfolgreich, und die Zertifikatsperrlisten werden erfolgreich heruntergeladen. Die Sperrprüfung schlägt jedoch in folgenden Fällen fehl:

```
No CRL found with matching CDP
revocation status = 2
```

Dieses Problem tritt auf, wenn der DMVPN-Hub-Router mehrere Download-URLs der Zertifikatsperrliste (Certificate Revocation List, CRL) verwendet, die auf dieselbe CRL-Datei verweisen. Die CRL-Download-Standorte umfassen sowohl IP-basierte als auch FQDN-basierte URLs, während das für die Spoke-Router ausgestellte Zertifikat nur die FQDN-basierte URL in seinem CRL Distribution Point (CDP) enthält.

Umwelt

- Cisco Geräte mit IOS® XE-Software, die für IPsec mithilfe der zertifikatbasierten IKE-Authentifizierung konfiguriert wurden
- Mehrere CRL-Download-Standorte mit IP- und FQDN-basierten URLs, die dieselben CRL-Dateien hosten.
- Das für die Peer-Geräte ausgestellte Zertifikat weist nur die eine URL im CDP auf.
- IPsec-Tunnelkonfiguration mit zertifikatbasierter Authentifizierung beim Erzwingen der Zertifikatsperrungsprüfung.

Auflösung

Die Lösung beinhaltet die Standardisierung auf eine einzelne kanonische CDP-URL in der PKI-Umgebung, um sicherzustellen, dass die URL während der CRL-Validierung exakt übereinstimmt.

Empfohlene Implementierungsschritte

1. Entfernen Sie IP-basierte URLs zum Herunterladen von Zertifikatsperrlisten aus der Hub-Konfiguration, wenn diese IP-basierten URLs nicht Teil des Zertifikat-CDP sind.

```
no crypto pki crl download url http://x.x.x.x/prod/Example%20Company%20Issuing%20CA1.crl
no crypto pki crl download url http://x.x.x.x/prod/Example%20Company%20Issuing%20CA2.crl
```

2. Konfigurieren Sie nur FQDN-basierte URLs zum Herunterladen von Sperrlisten, die mit dem CDP in den Spoke-Zertifikaten übereinstimmen.

```
crypto pki crl download url http://crl.examplecompnay.com/prod/Example%20Company%20Issuing%20CA1.crl
crypto pki crl download url http://crl.examplecompany.com/prod/Example%20Company%20Issuing%20CA2.crl
```

3. Erstellen von CA-Vorlagen aktualisieren, um konsistente CDP-URLs zu verwenden

Stellen Sie sicher, dass die ausstellenden CA-Vorlagen nur die FQDN-basierte CDP-URL in neu ausgestellte Zertifikate stempeln.

4. Erneute Anmeldung von Hub-and-Spoke-Zertifikaten (bei Änderung der CDP-URL)

Wenn Sie eine neue CDP-URL implementieren, ändern Sie die ausstellende Zertifizierungsstelle, um die neue CDP-URL zu veröffentlichen, und registrieren Sie die Hub- und Spoke-Zertifikate erneut, um die neue URL zu übernehmen.

Redundanzimplementierung

Damit die CRL-Anbieter-Redundanz beispielsweise dafür sorgt, dass dieselbe CRL an verschiedenen URL-Standorten veröffentlicht wird, um Fehler auf den Hostgeräten zu vermeiden, implementieren Sie die Backend-Redundanz hinter einem einzelnen FQDN mithilfe der folgenden Funktionen:

- DNS-Failover
- Load Balancer
- Redundante CRL-Infrastruktur

Verwenden Sie nicht mehrere CDPs mit unterschiedlichen Hostnamen/IPs, da diese von IOS XE als unterschiedliche CDPs behandelt werden, selbst wenn sie auf dieselbe CRL-Datei verweisen.

Verifizierung

Überprüfen Sie nach der Implementierung der Änderungen die CRL-Zwischenspeicherung und den Tunnelaufbau:

```
show crypto pki crl
```

Bestätigen Sie, dass die IKEv2-Sitzung erfolgreich eingerichtet wurde:

```
show crypto session details
```

Ursache

Das Problem wird durch das genaue Verhalten des CDP-URL-Abgleichs in IOS XE während der Sperrlisten-Validierung verursacht. Bei der Validierung eines Peer-Zertifikats, bei dem die Sperrfunktion aktiviert ist, führt IOS XE eine exakte Zeichenfolgenübereinstimmung zwischen der in das zu validierende Zertifikat eingebetteten CDP-URL und der im analysierten CRL-Cache des Hubs gespeicherten CDP-URL durch.

Diese Fehlersequenz tritt auf:

1. Der Hub lädt die Zertifikatsperrliste erfolgreich unter Verwendung der IP-basierten CDP-URL herunter und speichert sie intern unter dieser URL.
2. Spoke-Zertifikate referenzieren die FQDN-basierte URL im CDP.
3. Während der Sperrvalidierung sucht IOS XE nach einer zwischengespeicherten Sperrliste, die mit der FQDN-URL übereinstimmt.
4. Es wurde keine genaue Übereinstimmung gefunden, da IOS XE IP-basierte und FQDN-basierte URLs als unterschiedliche CDPs behandelt.
5. Der Router gibt "No CRL found with matching CDP" (Keine Sperrliste gefunden mit entsprechendem CDP) mit dem Sperrstatus = 2 zurück.
6. Fehler bei der Zertifikatvalidierung mit %PKI-3-CERTIFICATE_INVALID.

IOS XE normalisiert die verschiedenen URL-Formate (IP und FQDN) nicht als gleichwertig, selbst wenn beide identische CRL-Inhalte für denselben Herausgeber zurückgeben.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.