IOS XE-certificaatvalidatiefouten oplossen als gevolg van CDP-URL-mismatch met meerdere CRL-download-URL

Inhoud

uitgifte

Nadat extra URL-locaties voor CRL-downloads zijn toegevoegd aan een Dynamic Multipoint VPN (DMVPN)-hubapparaat, slagen sommige spaaktunnels er niet in om vast te stellen vanwege een mislukte IKE-onderhandelingsfout en de hub registreerde deze fout:

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

Hoewel de validatie van de certificaatketen slaagt en CRL's met succes worden gedownload, mislukt de herroepingscontrole met tussenpozen met:

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

Dit probleem treedt op wanneer de DMVPN-hubrouter meerdere downloadlocaties van de Certificate Revocation List (CRL) gebruikt die naar hetzelfde CRL-bestand verwijzen. De CRL-downloadlocaties bevatten zowel IP-gebaseerde als FQDN-gebaseerde URL's, terwijl het certificaat dat wordt uitgegeven aan de spaakrouters alleen de FQDN-gebaseerde URL in zijn CRL Distribution Point (CDP) heeft.

milieu

- Cisco-apparaten waarop IOS® XE-software is geconfigureerd voor IPsec met behulp van op certificaten gebaseerde IKE-verificatie.

- Meerdere CRL-downloadlocaties met zowel IP-gebaseerde als FQDN-gebaseerde URL's met dezelfde CRL-bestanden.
- Certificaat uitgegeven aan de peer-apparaten heeft alleen de ene URL in zijn CDP.
- IPsec-tunnelconfiguratie met behulp van op certificaten gebaseerde verificatie terwijl de controle op intrekking van certificaten wordt uitgevoerd.

resolutie

De resolutie omvat het standaardiseren van één canonieke CDP-URL in de PKI-omgeving om te zorgen voor exacte URL-matching tijdens CRL-validatie.

Aanbevolen implementatiestappen

1. Verwijder op IP gebaseerde CRL-downloadURL's uit de Hubconfiguratie als dergelijke op IP gebaseerde CRL-URL's geen deel uitmaken van de Certificate CDP

```
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. Configureer alleen CRL-downloadURL's op basis van FQDN die overeenkomen met de CDP in de Spoke-certificaten

```
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. Uitgevende CA-sjablonen bijwerken om consistente CDP-URL's te gebruiken

Zorg ervoor dat de CA-sjablonen die worden uitgegeven alleen de op FQDN gebaseerde CDP-URL in nieuw uitgegeven certificaten stempelen.

4. Hub- en spraakcertificaten opnieuw inschrijven (als u overschakelt naar een nieuwe CDP-URL)

Als u een nieuwe CDP-URL implementeert, wijzigt u de CA van afgifte om de nieuwe CDP-URL te publiceren en schrijft u zowel hub- als spaakkertificaten opnieuw in om de nieuwe URL te dragen.

Redundantie-implementatie

Voor redundantie van CRL-providers, bijvoorbeeld om hetzelfde CRL op verschillende URL-locaties te laten publiceren om te beschermen tegen storingen op de hostingapparaten, implementeert u backend-redundantie achter een enkel FQDN met behulp van:

- DNS-failover
- Load balancer
- Redundante CRL-infrastructuur

Gebruik geen meerdere CDP's met verschillende hostnamen/IP's, omdat IOS XE deze als verschillende CDP's behandelt, zelfs als ze naar hetzelfde CRL-bestand verwijzen.

Verificatie

Controleer na het implementeren van de wijzigingen de CRL-caching en tunnelinstelling:

```
show crypto pki crl
```

Bevestig dat IKEv2-sessie succesvol is ingesteld:

```
show crypto session details
```

Oorzaak

Het probleem wordt veroorzaakt door het exacte CDP-URL-matchinggedrag van IOS XE tijdens CRL-validatie. Bij het valideren van een peer-certificaat met herroepingscontrole-crl ingeschakeld, voert IOS XE een exacte tekenreeksovereenkomst uit tussen de CDP-URL die is ingebed in het certificaat dat wordt gevalideerd en de CDP-URL die is gekoppeld aan de CRL die is opgeslagen in de geparseerde CRL-cache van de hub.

Deze faalvolgorde treedt op:

1. Hub downloadt met succes CRL met behulp van een op IP gebaseerde CDP-URL en plaatst deze intern in een cache onder die URL.
2. Spoke-certificaten verwijzen naar de op FQDN gebaseerde URL in de CDP.
3. Tijdens de herroepingsvalidatie zoekt IOS XE naar een CRL in de cache die overeenkomt met de FQDN-URL.
4. Er is geen exacte overeenkomst gevonden omdat IOS XE IP-gebaseerde en FQDN-gebaseerde URL's als verschillende CDP's behandelt.
5. Router retourneert "Geen CRL gevonden met overeenkomende CDP" met herroepingsstatus = 2.
6. Certificaatvalidatie mislukt met %PKI-3-CERTIFICATE_INVALID.

IOS XE normaliseert verschillende URL-indelingen (IP versus FQDN) niet als equivalent, zelfs niet wanneer beide identieke CRL-inhoud retourneren voor dezelfde uitgever.

Gerelateerde inhoud

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.