Risoluzione degli errori di convalida dei certificati IOS XE causati da URL CDP non corrispondenti con più URL di download CRL

Sommario

Problema

Dopo aver aggiunto ulteriori percorsi URL di download CRL a un dispositivo hub DMVPN (Dynamic Multipoint VPN), alcuni tunnel spoke non vengono stabiliti a causa di un errore di negoziazione IKE e l'hub ha registrato questo errore:

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

Sebbene la convalida della catena di certificati abbia esito positivo e i CRL siano stati scaricati correttamente, il controllo delle revoche ha esito negativo in modo intermittente con:

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

Questo problema si verifica quando il router hub DMVPN utilizza più percorsi URL di download dell'elenco di revoche di certificati (CRL) che puntano allo stesso file CRL. I percorsi di download dei CRL includono sia URL basati su IP che URL basati su FQDN, mentre il certificato rilasciato ai router spoke contiene solo URL basati su FQDN nel relativo punto di distribuzione CRL (CDP).

Ambiente

- Dispositivi Cisco con software IOS® XE configurato per IPsec che utilizzano l'autenticazione IKE basata su certificato.

- Percorsi di download di più CRL con URL basati su IP e FQDN che ospitano gli stessi file CRL.
- Il certificato rilasciato ai dispositivi peer ha solo un URL nel relativo CDP.
- Configurazione del tunnel IPSec che utilizza l'autenticazione basata su certificato durante l'applicazione della verifica di revoca del certificato.

Risoluzione

La risoluzione prevede la standardizzazione su un singolo URL CDP canonico in tutto l'ambiente PKI per garantire una corrispondenza esatta dell'URL durante la convalida CRL.

Fasi di implementazione consigliate

1. Rimuovere gli URL di download dei CRL basati su IP dalla configurazione hub, se tali URL non fanno parte del CDP del certificato

```
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. Configurare solo gli URL di download dei CRL basati su FQDN che corrispondono al CDP nei certificati spoke

```
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. Aggiornare i modelli CA di emissione per utilizzare URL CDP coerenti

Verificare che i modelli della CA di emissione contrassegnino solo l'URL CDP basato su FQDN nei nuovi certificati rilasciati.

4. Registrare nuovamente i certificati Hub e Spoke (se si passa al nuovo URL CDP)

Se si implementa un nuovo URL CDP, modificare l'autorità di certificazione emittente in modo che pubblichi il nuovo URL CDP e registrare nuovamente i certificati hub e spoke in modo che includano il nuovo URL.

Implementazione della ridondanza

Per la ridondanza del provider CRL, ad esempio, affinché lo stesso CRL venga pubblicato in percorsi URL diversi per la protezione da errori sui dispositivi host, implementare la ridondanza back-end dietro un singolo FQDN utilizzando:

- failover DNS
- Bilanciamento del carico
- Infrastruttura CRL ridondante

Non utilizzare più CDP con nomi host/IP diversi, in quanto IOS XE li tratta come CDP diversi anche se fanno riferimento allo stesso file CRL.

Verifica

Dopo aver implementato le modifiche, verificare la memorizzazione nella cache CRL e la definizione del tunnel:

```
show crypto pki crl
```

Confermare che la sessione IKEv2 sia stata stabilita correttamente:

```
show crypto session details
```

Causa

Il problema è causato dal comportamento esatto della corrispondenza URL CDP di IOS XE durante la convalida del CRL. Quando si convalida un certificato peer con CRL di controllo delle revoche abilitato, IOS XE esegue una corrispondenza esatta tra l'URL CDP incorporato nel certificato da convalidare e l'URL CDP associato al CRL archiviato nella cache CRL analizzata dell'hub.

Si verifica la seguente sequenza di errori:

1. L'hub scarica correttamente il CRL utilizzando l'URL CDP basato su IP e lo memorizza nella cache internamente in tale URL.
2. I certificati spoke fanno riferimento all'URL basato su FQDN nel relativo CDP.
3. Durante la convalida di revoca, IOS XE cerca un CRL memorizzato nella cache corrispondente all'URL del nome FQDN.
4. Non viene trovata alcuna corrispondenza esatta perché IOS XE tratta gli URL basati su IP e FQDN come CDP diversi.
5. Il router restituisce "No CRL found with matching CDP" (Nessun CRL trovato con CDP corrispondente) con stato di revoca = 2.
6. Convalida del certificato non riuscita con %PKI-3-CERTIFICATE_INVALID.

IOS XE non normalizza formati URL diversi (IP e FQDN) come equivalenti, anche se entrambi restituiscono contenuto CRL identico per lo stesso emittente.

Contenuto correlato

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).