حل حالات فشل التحقق من صحة شهادة IOS XE بسبب عدم تطابق عنوان URL الخاص ب CRL المتعدد لتنزيل URL عنوان مع CDP

المحتويات

مسألة

بعد إضافة مواقع عنوان URL لتنزيل CRL الإضافية إلى جهاز موزع Dynamic Multipoint VPN (DMVPN)، فشلت بعض الأنفاق التي تم التحدث فيها في الإنشاء بسبب فشل تفاوض IKE وقام الموزع بتسجيل هذا الخطأ:

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

على الرغم من نجاح التحقق من صحة سلسلة الشهادات وتنزيل قوائم التحكم في الوصول (CRL) بنجاح، إلا أن التحقق من الإبطال يفشل بشكل متقطع مع:

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

تحدث هذه المشكلة عندما يستخدم موجه لوحة وصل DMVPN عدة مواقع لعنوان URL لتنزيل CRL نفسه. تتضمن مواقع تنزيل CRL قائمة إبطال الشهادات (CRL) التي تشير إلى ملف CRL، بينما تحتوي كل من عناوين URL المستندة إلى FQDN وعناوين FQDN المستندة إلى IP على عنوان URL المستند إلى FQDN في الشهادة الصادرة للموجهات التي يتحدث بها فقط على عنوان URL الخاص بها لنقطة توزيع CRL (CDP).

البيئة

- أجهزة Cisco التي تشغل برنامج IOS® XE الذي تم تكوينه ل IPsec باستخدام مصادقة IKE المستندة إلى الشهادة.

- مواقع تنزيل CRL متعددة مع عناوين URL المستندة إلى IP وتلك المستندة إلى FQDN التي تستضيف ملفات CRL نفسها.
- تحتوي الشهادة التي تم إصدارها للأجهزة النظيرة على عنوان URL واحد فقط في بروتوكول CDP الخاص بها.
- تكوين نفق IPsec باستخدام المصادقة المستندة إلى الشهادة أثناء تنفيذ التحقق من إبطال الشهادة.

قرار

يتضمن الحل توحيد المعايير على عنوان CDP واحد قانوني عبر بيئة PKI لضمان مطابقة عنوان URL بدقة أثناء التحقق من صحة CRL.

خطوات التنفيذ الموصى بها

1. إزالة عناوين CRL المستندة إلى IP لتنزيل URL من تكوين لوحة الوصل، إذا كانت عناوين CRL المستندة إلى IP ليست جزءا من بروتوكول CDP للشهادة

```
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. قم فقط بتكوين عناوين CRL لتنزيل CRL المستندة إلى FQDN التي تطابق CDP في الشهادات التي تم التحدث بها

```
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. تحديث قوالب المرجع المصدق الإصدار لاستخدام عناوين CDP URL المتسقة

تأكد من ختم قوالب المرجع المصدق للإصدار فقط عنوان URL لبروتوكول CDP المستند إلى FQDN في الشهادات الصادرة حديثا.

4. إعادة تسجيل الشهادات المحورية والشهادات التي تم التحدث بها (إذا تم تغيير عنوان URL لبروتوكول CDP الجديد)

في حالة تنفيذ عنوان CDP جديد، قم بتغيير المرجع المصدق الخاص بالإصدار لنشر عنوان URL الجديد لبروتوكول CDP وإعادة تسجيل كل من الشهادات المحورية والشهادات التي يتم التحدث بها لحمل عنوان URL الجديد.

تنفيذ التكرار

بالنسبة لموزع CRL الاحتياطي، على سبيل المثال، لنشر نفس CRL في مواقع URL مختلفة للحماية من حالات الفشل على الأجهزة المضيفة، قم بتنفيذ تكرار الطرف الخلفي خلف FQDN واحد باستخدام:

- تجاوز فشل DNS
- موازن التحميل
- بنية CRL الأساسية المكررة

تستخدم العديد من بروتوكولات CDP ذات أسماء المضيف/IPs المختلفة حيث يتعامل IOS XE مع هذه على أنها وحدات CDP مختلفة حتى إذا كانت تشير إلى نفس ملف CRL.

التحقق

بعد تنفيذ التغييرات، تحقق من التخزين المؤقت ل CRL وإنشاء النفق:

```
show crypto pki crl
```

تأكد من أن جلسة عمل IKEv2 تؤسس بنجاح:

```
show crypto session details
```

السبب

سبب المشكلة هو سلوك IOS XE لمطابقة عنوان URL لبروتوكول CDP أثناء التحقق من صحة CRL. عند التحقق من صحة شهادة نظير مع تمكين ميزة إبطال-فحص CRL، يقوم IOS XE بإجراء تطابق تام للسلسلة بين عنوان URL لبروتوكول CDP المدمج في الشهادة وعنوان URL لبروتوكول CDP المقترن ب CRL المخزن في ذاكرة التخزين المؤقت ل CRL التي تم تحليلها في الصرة.

يحدث تسلسل الفشل هذا:

1. يقوم Hub بتنزيل CRL بنجاح باستخدام CDP URL المستند إلى IP ويتخزينه داخليا ضمن عنوان URL هذا.
2. تشير الشهادات التي تم التحدث بها إلى URL المستند إلى FQDN في CDP الخاص به.
3. أثناء التحقق من صحة الإبطال، يبحث IOS XE عن CRL مخزن مؤقتا يطابق URL FQDN.
4. لم يتم العثور على تطابق تام لأن IOS XE يتعامل مع عناوين URL المستندة إلى IP و FQDN على أنها بروتوكولات CDP مختلفة.
5. يقوم الموجه بإرجاع "لم يتم العثور على CRL مع CDP المتطابق" مع حالة الإبطال = ?
6. يفشل التحقق من صحة الشهادة مع وجود PKI-3-CERTIFICATE_INVALID٪

لا يقوم IOS XE بتطبيع تنسيقات URL المختلفة (IP مقابل FQDN) على أنها مكافئة، حتى عندما تقوم كلتاهما بإرجاع محتوى CRL متماثل لنفس المصدر.

المحتوى ذي الصلة

- [الدعم الفني والتنزيلات من Cisco](#)

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).