دليل عدم الثقة في Cisco IOS XE و GuestShell CA Trust Media

المحتويات

الغرض

يوفر هذا المستند إرشادات لـ Cisco IOS® XE لفقدان الثقة في حالات الطوارئ لسلطات الشهادات الوسيطة والجذور الإلكترونية.

أستخدم هذا الدليل لمراجعة ثقة CA وإدارتها للخدمات التي يسمح تكوينها بالتدرجات الهرمية المتأثرة. يتم تحديد إمكانية تطبيق المنتج والمعالجة المطلوبة في معلومات Cisco. تحقق من دعم الأمر وتأثير الخدمة لإصدار Cisco IOS XE الخاص بك قبل تغيير الثقة.

معلومات Cisco: cisco-sa-emudhra-info-scS22A1r

شهادات التوثيق (CA) المتأثرة: الأصل والتوقيع المتبادل

تم التحقق من المخزون في 29 أكتوبر 2026. وتتأثر ثمانية مفاتيح CA التي تصدرها eMUDHRA بما يلي: ستة من أجل TLS واثنتان من أجل توقيع الرمز. يظهر كل مفتاح في شهادة مرجع مصدق أصلية صادرة عن مصنف emSign وشهادة مرجع مصدق موقع تبادلي من Sectigo. وبالتالي، يحتوي المخزون على 16 شهادة: 12 ترخيص TLS و 4 شهادات توقيع كود.

ولكل زوج أصلي/متشارك الموقع نفس الموضوع والمفاتح العام، ولكن له مصدر مختلف ورقم تسلسلي وبصمة شهادة SHA-256. ويوفر النمطان مسارات اعتماد بديلة ويجب تضمين كل النمطين في مراجعة الحسابات.

ألف - الجهات المصدرة والشهادات المتأثرة

المصدر A — شهادات TLS الأصلية: CN=emSign Root TLS CA - G3، O=eMudhra Technologies Limited، C=in.

المصدر B — شهادات توقيع الكود الأصلية: CN=emSign Root CS CA - G3، O=eMudhra Technologies Limited، C=IN.

المصدر C — جميع الشهادات الموقعة: CN=AAA Certificate Services، o=Comodo CA Limited،

l=Salford، st=Greater Manchester، c=GB (Sectigo).

مواضيع G3B: O=Edhra BV، C=NL. مواضيع G3C: O=Edhra Inc، C=US. وتسرد كل خلية
مخ تلفة مرا جع م صدره ا، وال م سلسل ال سدا سي ال عشري، وب صمة ال ألص ابع SHA-256 (سطران).
ال ي غير ال حد ال صفري ال بادئة ق يمة تسلسلية.

CA الإصدار المتأثر (CN)	الشهادة الأصلية المصدر / التسلسل (hex) / SHA-256	شهادة SECTIGO ذات التوقيع التبادلي المصدر / التسلسل (hex) / SHA-256
1. EM DV TLS CA - G3B TLS	المصدر ألف A4AEE678F23362B4C0E460B772F214 42C4ACCD12C4F59597925E1A08A7A901 02608543809308D50EC427E118BA1493	المصدر C A024FDF4BA665C785CE4A020483858B7 45A883F349AEDFD5F3A649B5498FFB12 1712BA8B448F3F2A91DBC5A766FCDDBE
2. EM OV TLS CA - G3B TLS	المصدر ألف 6CADA367FB1C100088120EA202D568 98B896625C0c230ADEEC3EB2CF6AAD50 01ECF9156A68644e82374CE5833bc25b	المصدر C E94223BDE92F914E5AB9ACABFDAC3710 5F1DED4DD590AF74631290CF073b122a 2AAC6A1FA479778A0BD43579BD832699
3. EM EV TLS CA - G3B TLS	المصدر ألف C7C41EFE92D825F05EAE841A4A82C1 E7568FE6E12331F4FD7DE61DA4C7559D 0F8EB192A218D4741A3BA75184333838	المصدر C D8F8685E4F2BD9D82402A85A1C1EB731 579480aea166290BD3C643589E795FC0 D0E54e86505D180F1DFF99EFD3199512
4. EM DV TLS CA - G3C TLS	المصدر ألف 588B2E3C2BB8CDA13E1A1209254321 0164D7CEAE5BB909C272AF151FF44B11 77AE9B47D9424B94F1D9558C30934D19	المصدر C 91F347F1A5B7D39962B95E0EE4E299D1 62B7F9868263F72F6911FC78CEAF72C1 979158b7368bf648683bb2aa39b02e72
5. EM OV TLS	المصدر ألف	المصدر C

CA رادصإلا رثأتملا (CN)	ةيلصألا ةداهشلا لسلستلا (hex) / SHA-256 / ردصملا	ةداهش SECTIGO ذاتلا عيقوتلا يلباتلا لسلستلا (hex) / SHA-256 / ردصملا
CA - G3C TLS	296926C227A3A1526392B19482A504 CB6E15165AC802E9B3F993F16C25D41F 4E81C21EBDE71AE1B012AC00BF9C7C3F	8D5A4811939EF447D77111CDD9849AE9 7485B51C0ED192878FA1D2F948FB529A E1842CC5086C4B67F7BE5B2039DE9489
6. EM EV TLS CA - G3C TLS	فلأ ردصملا 8009928a64107601AF05FA2F19F109 432EC25F0D28DE9006D97BF752F17BBB 2CD41F669933FCB072D9A1148D0261F3	C ردصملا 05F078752DECE7A1BB8595D303167171 FD9D5C2DBBD4995AB69B8D50C439D952 7B00529199C2FD01B2174EB58F07021F
7 - EM OV CS CA - G3B عيقوت دوكلا	عاب ردصملا 7818933F8F85B4619a2B35FBA83d0a 9E39DE2881273ACC225A149C72BA3E0F 5142496369AB633EE1DC7DF5DB067B4	C ردصملا 41e32b73ac185d6CE0d7480bacf84e69 A496E23AC0CAB8155FC9B117B97EAE36 8EFCBB9041AEC8804D5A308D2D01C2D8
8 - EM OV CS CA - G3C عيقوت دوكلا	عاب ردصملا 544B7F922C31AE220A4A922916F6E6 4B2460A466F95FD40113BCDCCA2CEB29 B3B093921DE45474DA7DF48874C630B1	C ردصملا D6A5EF613B390F32EF9CDF349F772841 84112972B8E59D14560AE7E711965447 4AAD11990CF3722BFC1E3B91615E1FD

زييمتلل تاداهشلا تاراسم - عاب

يلصألا TLS راسم

```
emSign ECC Root CA - G3
+-- emSign Root TLS CA - G3 (issued by emSign ECC Root CA - G3)
    +-- Original EM DV/OV/EV TLS CA - G3B or G3C
        +-- TLS identity certificate
```

مسار توقيع الرمز الأصلي (عنصر التحكم الجذر موثوق به مباشرة)

```
emSign Root CS CA - G3
+-- Original EM OV CS CA - G3B or G3C
+-- Code-signing identity certificate
```

مسار التوقيع المتقاطع Sectigo (TLS وتوقيع الرمز)

```
AAA Certificate Services
+-- One of the eight cross-signed CAs listed above
+-- TLS or code-signing identity certificate
```

هذا CA عندما يكون G3 - الجذر الخاص بتوقيع الجذر TLS ل CA عند TLS مسار إنهاء أيضا يمكن .موثوقا به مباشرة. تظهر الرسوم البيانية العلاقات المصدر ذات الصلة؛ يعتمد المسار المقبول على نقاط الربط الثقة وسياسة التحقق من الصحة للخدمة المستهلكة.

يوفر المرجع المصدق الأصل/الجذر الموضح مثال سياق السلسلة والتي تم حسابه بين مفاتيح الإصدار الثمانية التي تم إختراقها. يكون القرار الخاص بإزالة أحد الوالدين/الجذر أو عدم الثقة فيه منفصل عن تحديد مفتاح وسيط تم تعريفه للخطر.

للتعريف، أستخدم مصدر الشهادة والرقم التسلسلي مع بصمة الإصبع SHA-256. اسم الموضوع وحده غير كاف. تحدد بصمة الشهادة متغير شهادة واحد؛ تحدد تجزئة SPKI SHA-256 المفاتيح العام المشترك بواسطة النماذج الأصلية والموقعة. ال تمنع إزالة الوسيط المخزن مؤقتا فقط النظير من تقديمه عبر مسار موثوق به متبقي.

المصادر وتاريخ التحقق

تم التحقق من هوية الشهادة مقابل مرفقات الأحداث العامة في 29 أكتوبر 2026. يحتوي كل زوج أصلي/متبادل التوقيع على نفس المفاتيح العام. أستخدم المعلومات المباشرة من Cisco لتطبيق المنتج وحالة المعالجة.

معلومات Cisco: cisco-sa-emudhra-info-scS22A1r

سجل حوادث موزيلا: تسوية رئيسية متوسطة (2083449)

مرفق شهادة CA الأصلي (9664066)

[مرفق شهادة AAA الموقع من خالل المصادقة والتفويض والمحاسبة (9664067)]

[قلجسملاو ةيلصألا TLS ةداهش تارادص :لبأ]

اعتبارا من 31 أكتوبر 2026، لم يتم تحديد EMsign Root CA - G1 ضمن CAs المعرضة للخطر. ستؤثر المؤسسات التي تستخدم هذه الجذور على الثقة المستمرة بها. يرجى مراجعة سياساتك والتحديثات الاستباقية.

كيفية إدارة Cisco IOS XE لثقة الشهادة

تحتفظ PKI المكونة بـ CA/شهادات الهوية ونهج التحقق من الصحة. يحتوي PKI على شهادات CA مضمنة ومنزلة للخدمات التي تستخدمها. تحديد مصدر الثقة TrustPool وسياسة المستخدمة من قبل كل خدمة ذات صلة؛ الحل تغيير تجمع الثقة محل نقاط الثقة التي تم تكوينها بشكل منفصل.

1 - مراجعة الحسابات والإعداد

تحقق من إصدار البرنامج ووقت الجهاز والشهادات المثبتة:

<#root>

```
show version show clock show crypto pki trustpoints show running-config | section crypto pki trustpoint
```

قارن مصدر الشهادة الكامل والرقم التسلسلي السداسي العشري مع المخزون، باستخدام SHA1 فقط، لا MD5 و Cisco IOS XE بصمات الأصابع. حيث يعرض الموضوع كسياق داعم. يمكن مقارنة بصمات الأصابع SHA-256 للمخزون مباشرة في هذا الإخراج؛ يتم توفيرها للتحقق من ملفات الشهادات خارج الجهاز. يمكن أن تختلف مسافة البادئة 00 في الأرقام التسلسلية. تحدد عمليات البحث عن أسماء الموردين المرشحين فقط. قم بتسجيل الخدمات التي تعتمد على كل نقطة ثقة وتحقق من المسارات الأصلية والموقعة، بما في ذلك الوسائط الموثوق بها مباشرة.

الأمثلة: المرجع المصدق الجذر والنموذج الفرعي المتأثر

يتم عرض أمثلة مختصرة من شهادة السرعة؛ يتم حذف الحقول الأخرى. قارن الموضوع، المصدر والرقم التسلسلي.

مثال المرجع المصدق الجذر: EmSign ECC Root CA - G3

```
CA Certificate
Certificate Serial Number (hex): 3CF607A968700EDA8B84
Issuer:
cn=emSign ECC Root CA - G3
Subject:
cn=emSign ECC Root CA - G3
Associated Trustpoints:
```

مثال SubCA المتأثر: شهادة أصلية صادرة عن emSign

```
CA Certificate
Certificate Serial Number (hex): 00A4AEE678F23362B4C0E460B772F214
Issuer:
cn=emSign Root TLS CA - G3
Subject:
cn=EM DV TLS CA - G3B
Associated Trustpoints:
```

مثال SubCA المتأثر: شهادة SECTIGO ذات التوقيع التبادلي

```
CA Certificate
Certificate Serial Number (hex): 00A024FDF4BA665C785CE4A020483858B7
Issuer:
cn=AAA Certificate Services
Subject:
cn=EM DV TLS CA - G3B
Associated Trustpoints:
```

يحتوي كل النمطين SubCA على نفس الموضوع ولكن مع أختلاف الإصدارات والمسلسلات. مطابقة المصدر الكامل والمسلسل بالمخزون؛ يمكن أن تختلف المسافة البادئة بين الجذر الحروف 00. تسجيل TrustPoints المقترنة لتحديد موقع TrustPoint أو التجمع المالك. الظاهر هو سياق السلسلة؛ ليس واحدا من ثمانية مفاتيح إصدار إصدار مخالفة.

الاحتفاظ بأسلوب الوصول إلى الاسترداد وتوافر حزمة إستبدال معتمدة. أستخدم إجراء النسخ الاحتياطي للشهادة/المفاتيح المعتمد عند الحاجة. انسخ التكوين إحتياطي؛ هذه النسخة وحدها ليست نسخة إحتياطية لمفاتيح خاصة:

<#root>

```
copy running-config
```

استبدل مواضع الأقواس المؤقتة بقيم معتمدة خاصة بالجهاز. أستخدم نظام الملفات المطلوب أو bootflash: أو flash:، مثل show file أنظمة المضمنة.

2. مراجعة مسارات الثقة

إزالة CAs الفرعية المتأثرة الموثوق بها مباشرة

قم بإزالة SubCAs الموثوق بها مباشرة من نقاط الثقة ومجموعات مصادر الثقة التي تم تنزيلها. لا تعتمد على إعدادات الإبطال لتخطي الثقة المباشرة في مرجع مصدق تم إختراقه.

إزالة المرجع المصدق الجذر الاختياري

تعد إزالة المرجع المصدق الجذري بمثابة توصية إختيارية لتوفير حماية إضافية. يمكن أن يبقى الجذر المطلوب موثوقا به عندما تحصل عمليات فحص الخدمة الفعلية CRL/OCSP على الحالة الحالية، وتقييم SubCA المتأثرة تحت أصل موثوق به، وترفض السلاسل والتحقق، والأصلية المتأثرة، والموقعة التبادلية، والسلاسل الأطول القابلة للتطبيق. في ظل هذه الظروف، يوفر التحقق من الإبطال الحماية من المصدرين الذين تم تحديدهم المعرضين للخطر دون حذف الجذر من الفشل إذا لم توفر أي من الطريقتين المكونتين حالة قابلة للاستخدام.

فكر في إزالة نقاط الربط غير الضرورية بين الجذر/الثقة لتقليل الاعتماد على خدمات AAA إلى الوراء: يمكن أن تؤدي إزالة خدمات شهادات AAA إلى إلغاء المستخدم. تقييم تبعيات الخدمة. قم بتغطية كل من مساري AAA و eModhra. مقاطعة السلاسل الشرعية غير المرتبطة. يؤدي حذف SubCA المخزن مؤقتا فقط إلى حظر نسخة مقدمة من قبل نظير من خلال أصل موثوق به باق.

إزالة نقطة موثوق بها محددة

بالنسبة لنقطة الثقة التي قام المسؤول بتكوينها والتي تم تحديدها لإزالتها:

```
<#root>

configure terminal no crypto pki trustpoint
```

```
end
```

اذا .امهاب قرتقملا تاداهشلا ريدصت ىلإ TrustPoint ةلازإ يدؤي .لوبقلا لبق ديكأتلا ةعجارم
كاذ ،لدابتسلإ جاحلا ىلإ هجاوزلا تناك ،لدابتسلإ قباطم حيتافم لجأللا ةزهجلا
ةمدخلا ليجست ءارجإ مادختساب هب صاخلا ةمدخلا طبر ثيدحتب موقم .ةداهش تيبثت يدؤي
.هجاوزلا هيوتسلإ ديدج ردصم عجرم

لدابتسلإ ةلمحلا مدختسأ ،ءارجإ ةمدختسملا تنزيلاو تلا تاداهشلا عمجت تاخالدإل
.Cisco نم TAC هيجوتو عوضوملا جتنملا ثيدحت تازيملا ربع ةرادلا وأ ةجمدملا

3. ثيدحت TrustPool الذي تم تنزيله، إذا لزم الأمر

.يلاتلا ةوطخلا يف اهنم ققحتلا مت بولطملا رذجلا/لصألا ىلإ ةدنتسملا ةقثلا تاطلس
.لدابتسلا اهتيلمع ءانثأ اهيلإ ةجاحلا ةلزانملا ةلدألا ةعومجم ىلع ظافحلا ىجري

3.1 تحقق مما إذا تم تثبيت حزمة تم تنزيلها واستخدامها

```
<#root>

show running-config | section crypto pki certificate pool show crypto pki trustpool verbose show crypto
```

ةداهش عيمجت تحت ةلجسملا تاداهش PKI ةفشرملا و CA تاعجرملا عضو تم يتلا تاداهشلا
ios.p7b نم ةلزانملا تافلم ءامسأ فلتخت نأ نكمي .ليزنتلا تم :اهيلع TrustPool
ةثبملا فلملا نزخملا وأ URL صاخلا باسحلا ثيدحت ذيلا تم نيوكتها فقط .ios_core.p7b
ةمدخلا ليجست ءارجإ مادختساب ةمدخلا بتأكيد موقم .ةمدخلا هذه لبق نم ةقثوم وأ
.ثرأتملا نزخملا باهنا ةصاخلا CA تاداهش نارقو .ليزنتلا ،ةمدخلا هذه لبق نم ةقثوم
.ىرخألا ةقثلا رداصم ميقي لازي ال ؛لدابتسلاو ليطعتلا طخي موقم ،

3.2 تنظيف تجمع الثقة الذي تم تنزيله

.ليطعتلا لبق ةدمتعم ةداهش عيمجتو ةداهشلا داريتسا ىلإ لوصولا باظافحلا
.ةعباتلا تامدخلا ليطعتل طيطختلا .ةقثلا ةلازإ ىلع دمتعي لقنلا كاذ اذإ كلذ دعب ليزنتلا

<#root>

```
configure terminal crypto pki trustpool clean end
```

```
show crypto pki trustpool verbose
```

تأكيد فقدان سجلات CA التي تم تنزيلها. يزيل التنظيف كل شهادات TrustPool التي تم تنزيلها وملفات الحزمة المدارة الخاصة بها؛ وتظل بطاقات الائتمان المتكاملة المتكاملة ونقاط الثقة المنفصلة قائمة. ال تقم بالحفظ حتى تنجح عمليات التحقق من الاستبدال والخدمات.

3.3 الحصول على حزمة الاستبدال المعتمدة وتثبيتها

الحصول على حزمة موقعة من Cisco معتمدة. حدد IOS.p7b أو ios_core.p7b للخدمات المطلوبة وتأكد من أنه يستثني الشهادات المتأثرة ومراسي الثقة غير المرغوب فيها المحددة أعلاه. تحتوي الحزم القديمة التي تم فحصها في 31 أكتوبر 2026 على CA - G1 في ios.p7b، ولكن ال تحتوي على eMudhra أو AAA Certificate Services CA في ios_core.p7b. يحتوي Core على مجموعة ثقة أصغر: تحقق من تبعيات الخدمة قبل التحويل، وتحقق من محتويات الحزمة التي تقوم بتثبيتها. قم بتشغيله خارج تخزين TrustPool المدار باستخدام نقل HTTPS أو SCP المعتمد.

حزمة CA الكاملة من Cisco: ios.p7b

حزمة CA الأساسية من Cisco: ios_core.p7b

<#root>

```
show file systems copy
```

```
configure terminal crypto pki trustpool import url
```

```
end show crypto pki trustpool verbose
```

على سبيل المثال، يمكن أن يكون URL المرحلي flash:approved-ios.p7b. إذا فشل الاستيراد، قم باستعادة حزمة معتمدة قبل الحفظ. تحقق من CAs المقصودة والاتصالات المطلوبة. قم بتنظيف ليس قائمة فارغة للشهادة: تأكيد النقاط الموثوق بها المتبقية، رفض الإبطال المتأثرة من خلال السلاسل البديلة والمسارات المدمجة (CA) للتحكم بالوصول القسري أو إزالة مسار الثقة.

4. تكوين نهج التحديث والتحقق من الصحة

قبل إجراء التغييرات، قم بتسجيل نهج تجمع الثقة الموجود، ونهج TrustPoint المتأثرة، وارتباطات تعيين الشهادات، وعناوين URL للتحديث حتى يمكن استعادتها عند الحاجة.

لنقاط الثقة ذات الصلة التي تم تكوينها:

```
<#root>

configure terminal crypto pki trustpoint

revocation-check crl ocsp exit end
```

بالنسبة للخدمات التي تستخدم سياسة تجمع الثقة:

```
<#root>

configure terminal crypto pki trustpool policy chain-validation revocation-check crl ocsp exit end show
```

درس باص الخاص OCSP عنوان إلى عرضوم TrustPool جهن صحف نم قحتلا رارمتسإ نم قحتلا
لشف ي. رفوتم ريغ CRL دارتسإ نوكي امدنع OCSP لواحيو الوأ CRL زاهجلا لواحي والجذ.
عيش ال مقإ ةفاضإ ب مأتم ةرثأتم ةداهشلا ميقيت دنع ةغلملا ةجيتنلا صحف نم قحتلا
.عنمي نوكي لاطبإلا لانجا مطولبا.

نكمي يتلاو CA ةطساوب اهرشن تي تلاحلل ةيهانلا طاقنو حيحصلا تقولا نم قحتلا
لوصولا ،وتنسيقاتا ةجابتسالا ةلوبقملا ،مدعو دوجو إستثناءات إلغاء ةلباق
ةطيبتلل. ي جب تقييم حالة SubCAs ةرثأتم تحت أصل موثوق به. ي مكن للثقة
ةمدخلا رشابم في SubCA إيقاف ةحتلا قبل ةحتلا نم أصلها. تحقق من حصول الخدمة
ةلفعلي ةعلى الحالة الحالية القابلة للاستخدام ورفض السلاسل المتأثرة. إذا تعذر
ةحتلا نم صحف سلوك الوصول إلى خادم الحالة ورفض، فإن تعامل التكوين وحده على أنه
ةحتلا نم صحف سلوك الوصول إلى خادم الحالة ورفض، فإن تعامل التكوين وحده على أنه
حماية وثيقة؛ قم بإزالة مسارات الثقة ذات الصلة حيثما تطلب ذلك خطة التخفيف الخاصة
.بك. قم بإضافة أي شعيرة تجاوز حالة عدم التوفر

تحديث قوائم التحكم في الوصول إلى CRL المخزنة مؤقتا قبل التحقق من الحماية

يمكن إعادة إستخدام قائمة التحكم في الوصول (CRL) القابلة للاستخدام بالفعل في
ذاكرة التخزين المؤقت/قاعدة البيانات المحلية حتى بعد أن يقوم CA بنشر قائمة تحكم
في الوصول (CRL) أحدث. تحقق من إمكانية الوصول إلى خادم الحالة، ثم قم بمسح قوائم
:التحكم في الوصول (CRL) القديمة قبل التحقق من الحماية

<#root>

```
show crypto pki crls clear crypto pki crl show crypto pki crls
```

يقوم الأمر clear بإزالة قوائم التحكم في الوصول (CRL) المحلية لكافة نقاط الثقة؛ ال
وأ جديد توصيل البدائل. تأكد من انتهاء الإدخالات القديمة، ثم أبدأ توصيل جديد
يقوم بنفسه بتنزيل البدائل. قم بتشغيل show crls crypto pki مرة أخرى تحقق من صحة
الشهادة في الخدمة المتأثرة. و LastUpdate و NextUpdate وتقنطة التوزيع المقابل المنشور
وتحقق من كل مصدر ذي صلة متأثر، وليس فقط SubCA يغطي الذي الأصلي المصدر CRL
الحالي لـ CAs. قم بتضمين CRL المصدر المتأثرة. قد يؤثر المسح بشكل مؤقت
مصدر شهادات المعرف. تأكد رفض السلاسل المتأثرة؛ الاحتفاظ بالتحقق من صحة الفشل
.على الاتصالات الجديدة أثناء إحضار بيانات الحالة

مراجعة مصدر تحديث الحزمة

بالنسبة للأجهزة المتصلة، قم بشكل إختياري بتكوين مصدر تحديث الحزمة المعتمدة
:على انتهاء الصلاحية

<#root>

```
configure terminal crypto pki trustpool policy cabundle url
```

```
exit end show crypto pki trustpool policy
```

راجع جميع مصادر الحزم التي تم تكوينها. لا يستبدل التحديث المستند إلى انتهاء الصلاحية تحديث أمان فوري ويجب ألا يقوم باستعادة مسار ثقة غير مرغوب فيه.

مرشح تعيين الشهادة الاختياري: التغطية والحد

يتطابق مخطط شهادة Cisco IOS XE (cert-map) مع سمات الشهادة، مثل اسم المصدر. كتدبير إضافي، يمكن أن يساعد المرشح على رفض شهادات المعرف (الورقة) الصادرة مباشرة عن المراجع المصدقة الثمانية المدرجة. راجع نهج شهادات المطابقة الموجودة لنقاط الثقة قبل تطبيقها.

تم إختبار السلوك في 29 تشرين الأول/أكتوبر 2026 باستخدام هويات مختبرية في إطار PKI، على EM DV TLS CA - G3B أجهزة مختبرية تجريبية. في التحقق من صحة شهادة نظير تم إصدارها من خلال سلطة التصفية هوية تم إصدارها مباشرة ولكنه لم يمنع هوية مزورة غير شرعي مصدر مدرج. أستخدمت التغطية السلوكية SubCA إضافي؛ تم تأكيد عامل المؤقتة لعزل عامل المصادقة الإطلاق فقط على نقاط الثقة المعامل إلى تعطيل مصدر متأثر، مع الإصدارات الأخرى عامل التصفية. لم يتم التحقق من صحة إرشادات التطبيق والإصدارات الأخرى عامل التصفية هذه؛ اختبر الخدمة الفعلية قبل الاعتماد عليها.

<#root>

```
configure terminal crypto pki certificate map EMSIGN-ISSUER-FILTER 10 issuer-name nc cn=EM DV TLS CA - G
```

```
match certificate EMSIGN-ISSUER-FILTER exit end
```

هنا، تعني الشرطة "ال تحتوي". الاحتفاظ بجميع الشروط الثمانية السالبة الخاصة باسم عامل التصفية هذا. يفشل المرشح مصدر مباشر مطابق لأي اسم مدرج في نفس الإدخال، والتسلسل 10: يجب أن تتطابق كافة الشهادات لتمرير المصدر.

يمكن أن يعرض Cisco IOS XE الإدخالات العادية، على سبيل المثال، Issuer-name nc cn = em dv tls ca - g3b. كان تنسيق المسافات والمسافات الصغيرة هذا موجودا في الاختبار والتي تحتوي على مسافات إضافية. تأكيد الخريطة وربطها بنقطة الثقة الخاصة بالتحقق من الصحة السلوكي:
تستخدمها الخدمة بالفعل:

<#root>

show running-config | section crypto pki certificate map show running-config | section crypto pki trustp

يوفر عامل التصفية قائمة أسماء مرجع مصدق (CA) على مستوى السلسلة. على سبيل المثال:

```
Trusted root CA
+-- Affected SubCA
+-- New child SubCA
+-- ID (leaf) certificate
```

مصدر شهادات المعرف هو المرجع المصدق الفرعي التابع الجديد، لذلك يحدد عامل تصفية اسم المصدر الخاص به المرجع المصدق المتأثر الأعلى في السلسلة. ولا تزال هناك عمليات تحقق أخرى، بما في ذلك القيود المفروضة على قانون المنافسة النزيهة والإبطال. أستخدم عامل التصفية هذا فقط كحماية إضافية إلى جانب التحقق من صحة الإبطال والإجراءات الاختيارية لإزالة الجذر في هذا الدليل. إختبار الشهادات المصدره مباشره، وشهادات الطفل الفرعي، والشهادات المشروعه مع الخدمه الفعليه.

4 الترا جع عن الخطوة

إستعادة طرق الإبطال المسجلة، وإعدادات التحقق من صحة السلسلة، وارتباطات خريطة الشهادات. قم بإزالة عناوين URL الخاصة بالتحديث التي تمت إضافتها بواسطة هذا الإجراء، ثم قم باستعادة أي عناوين URL سابقة تم تغييرها. يزيل هذا المثال عنوان URL الخاص بالتحديث الإضافي ويطبق المرشح فقط؛ الق يقوم باستعادة إعدادات النهج الأخرى:

<#root>

configure terminal crypto pki trustpool policy no cabundle url

exit

```
crypto pki trustpoint
```

```
no match certificate EMSIGN-ISSUER-FILTER exit end
```

اذه بتشغيل عمليات الإزالة هذه فقط حيث تمت إضافة عنوان URL والربط بواسطة قم باستعادته. قم بإزالة خريطة تم إستبدال ربط خريطة شهادة سابق، قم بإعادة. إذا تم الإنشاء حديثا فقط بعد التأكد من عدم وجود أي تكوين آخر يشير إليها.

ال تستخدم أي سياسة تشفير pki trustPool فقط عند إعادة التعيين إلى الإعدادات الافتراضية هي النتيجة المقصودة والموافق عليها. تقوم هذه العملية الواسعة لإعادة الضبط بمسح عناوين URL للتحديث التي تم تكوينها وإعادة تعيين التحقق من الإبطال إلى ال شيء؛ ال يقوم باستعادة النهج المخصص السابق. ال تقوم الترا جع عن النهج باستعادة الشهادات المحذوفة أو إرجاع الحزمة المثبتة أو إستعادة قوائم التحكم في الوصول إلى CRL التي تم مسحها. قم بإعادة التحقق من الخدمات المطلوبة ورفض سلسلة التأثير قبل الحفظ.

5. التحقق من الحماية والحفظ

- تأكد من رفض السلاسل الأصلية والموقعة التبادلية المتأثرة، بما في ذلك الوسيط المورد من قبل النظير. حيثما تكون السلاسل الأطول ذات صلة، تحقق من الرفض عندما يكون المرجع المصدق المتأثر أعلى في السلسلة.
- تأكد من أن الاتصالات الشرعية المطلوبة ال تزال تعمل وأن أي هوية بديلة مرتبطة بالخدمة المقصودة.
- التحقق من السلوك عند عدم توفر بيانات الإبطال. لم يتم التحقق من صحة جلسات دمج TLS/IPsec تلقائيا بواسطة تغيير النهج؛ أستخدم إجراء إعادة الاتصال المعتمد للخدمة عند الحاجة.

بعد نجاح التحققات:

<#root>

```
show crypto pki certificates verbose show crypto pki trustpool policy write memory
```

تحقق من الثبات بعد إعادة التحميل المخططة التالية، حيثما أمكن، على الجهاز الاحتياطي. إن تختلف النتائج من نهج الثقة الموقوع، احتفظ بالسجلات واتصال cisco TAC قبل النظر في تغييرات الثقة التي تم التحقق منها.

قراءة اضافية

[إدارة جديرة بالثقة لـ Cisco IOS XE PKI]

[Cisco: تكوين الشهادات الموقعة من CA باستخدام Cisco IOS XE PKI]

[Cisco: التحقق من التخزين المؤقت لـ CRL وإبطاله]

دليل ثقة Cisco IOS XE GuestShell CA

الخطوة 1: تدقيق حالة نشر GuestShell للجهاز

يجب إجراء المعالجة فقط على أنظمة Cisco IOS XE التي تم تثبيت GuestShell بها وفي حالة التشغيل أو النشر. إذا كان GuestShell في حالة النشر، فيجب تمكينه أولا باستخدام الأمر 'guestshell enable' قبل تنفيذ أوامر الإصلاح. إذا كان إظهار قائمة إستضافة التطبيقات يشير إلى 'لم يتم العثور على تطبيق' (لم يتم نشر GuestShell أو تمكينه)، فلا يتطلب الأمر أي إجراء على GuestShell.

A. GuestShell في حالة النشر (الإجراء المطلوب: يجب التمكين أولا)

عند عرض قائمة إستضافة التطبيقات تقارير GuestShell في حالة النشر، يكون تخزين الحاوية GuestShell موجودا ولكن يتم إيقاف الحاوية. يجب تشغيل 'guestshell enable' قبل إدخال base (و'guestshell disable' إختياريا بعد إكمال المعالجة في حالة العودة إلى حالة الإيقاف):

<#root>

Router#

show app-hosting list

```
App id                                                  State
---------------------------------------------------------
guestshell                                              DEPLOYED
```

ب. GuestShell في حالة التشغيل (الإجراء مطلوب: مباشرة)

عند عرض قائمة إستضافة التطبيقات تقارير GuestShell في حالة التشغيل، يتم تشغيل GuestShell بشكل نشط ويمكن المتابعة مباشرة إلى وضع BASH:

```
<#root>

Router#

show app-hosting list

App id                                                  State
---------------------------------------------------------
guestshell                                              RUNNING
```

ب. لم يتم تمكين GuestShell / لم يتم نشره (لا يتطلب أي إجراء)

إذا كان إظهار قائمة إستضافة التطبيقات يشير إلى عدم العثور على أي تطبيق، فإن GuestShell غير مثبت أو غير ممكن على النظام، ولا يتطلب أي إجراء آخر:

```
<#root>

Router#

show app-hosting list

No App found
```

الخطوة 2: الوصول إلى GuestShell وتطبيق عدم ثقة المرجع المصدق

بالنسبة لـ Cisco IOS XE. إذا كان الإصدار يتضمن أمر EXEC ('enable') فقم بتنفيذ هذه الأوامر من وضع التكوين العام. ثم أدخل "سياسة الثقة الأساسية"، وقم بالتصعيد إلى الجذر، ثم قم بتكوين قائمة حظر CA باستخدام تحديد المجلد الديناميكي لضمان التوافق عبر جميع إصدارات Cisco IOS XE:

```
<#root>

! 1. If GuestShell is in DEPLOYED state, enable it first:
Router#
```

```
guestshell enable
```

```
! 2. Enter GuestShell bash shell:
Router#
```

```
guestshell run bash
```

```
! 3. Escalate to root user inside GuestShell:
[guestshell@guestshell ~]$
```

```
sudo -s
```

```
! 4. Prepare the ca-trust blocklist directory (compatible with 17.15.x and 17.18.x):
d=/etc/pki/ca-trust/source/blocklist
[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist
mkdir -p "$d"
```

التشكيك في شهادات eMudhra

قم بتنفيذ أوامر إستخراج الثقة الاستخراج كل شهادة eMohra تم إختراقها مباشرة إلى دليل إستخراج الثقة الاستخراج كل شهادة eMohra تم إختراقها مباشرة إلى دليل ثم أعقب ذلك إعادة بناء مخزن ثقة النظام، CA-Trust لتحكم قائمة الحظر:

```
trust extract --overwrite --format=pem-bundle \
--filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-%20G3;type=cert' \
"$d/emSign_ECC_Root_CA_-_G3.pem"

trust extract --overwrite --format=pem-bundle \
--filter='pkcs11:object=Comodo%20AAA%20Services%20root;type=cert' \
"$d/Comodo_AAA_Services_root.pem"

trust extract --overwrite --format=pem-bundle \
--filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-%20C3;type=cert' \
"$d/emSign_ECC_Root_CA_-_C3.pem"

trust extract --overwrite --format=pem-bundle \
--filter='pkcs11:object=emSign%20Root%20CA%20-%20C1;type=cert' \
"$d/emSign_Root_CA_-_C1.pem"

update-ca-trust extract
```

الخطوة 3: التحقق من الشهادات التي لم يتم توزيعها في GuestShell

تحقق من ظهور الشهادات الأربع المستخرجة في نهج عدم ثقة/حظر النظام واستبعادها من نقاط ربط الثقة النشطة باستخدام أمر التحقق أدناه. يؤكد الأمر أن الشهادات مسجلة في نهج قائمة الحظر.

```
                                                                ###Verify with below command
[guestshell@guestshell ~]$ trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign
                                                          label: AAA Certificate Services
                                                                  trust: distrusted
                                                                category: authority

                                                                                  --
                                                         label: emSign ECC Root CA - C3
                                                                  trust: distrusted
                                                                category: authority

                                                                                  --
                                                         label: emSign ECC Root CA - G3
                                                                  trust: distrusted
                                                                category: authority

                                                                                  --
                                                             label: emSign Root CA - C1
                                                                  trust: distrusted
                                                                category: authority

                                                                                  --
                                                             label: emSign Root CA - G1
                                                                        trust: anchor
                                                                category: authority

                                                       Output will vary based on CentOS Stream version
                                                                   ###Verify CentOS Stream Version
                                                    [guestshell@guestshell ~]$ cat /etc/redhat-release
                                                                       CentOS Stream release 8

                                  OS                              CentOS Stream 8       CentOS Stream 9
                                        Directory                        blacklist only        blocklist
                                Result shown                    trust: blacklisted    trust: distrusted
```

الخطوة 4: إستمرارية الحالة ودورة حياة الحاوية

ملاحظة حول إستمرارية الحاوية: تستمر تعديلات عدم ثقة الشهادة هذه عبر عمليتي guestshell disable' و'guestshell enable' الموجودة على /etc/pki/ca-trust لأن إزالة تمهيد الجهاز وإعادة التخزين الثابت للحاوية.

في الحالة المنشورة (إن أمكن): إذا كان GuestShell موجودا في الحالة المنشورة، فعليك إرجاع GuestShell إلى حالته الأصلية وتم تمكينه فقط لتنفيذ إجراء عدم الثقة هذا، وتشغيل "Guestshell disable" من BaseH والخروج عن طريق إيقافها التي تم إنشاؤها بواسطة EXEC للمستوى المتميز IOS:

<#root>

```
[root@guestshell ~]#
```

exit

```
[guestshell@guestshell ~]$
```

```
exit
```

```
Router#
```

```
guestshell disable
```

إعتبار مهم لدورة الحياة: إذا تم تدمير GuestShell بالكامل باستخدام 'Guestshell Destroy'، فسيتم إزالة نظام ملفات الحاوية. إذا تم إعادة تمكين GuestShell فيما بعد، تتم إعادة إنشاء الحاوية من صورة النظام الأساسي ويجب إعادة تطبيق خطوات إصلاح عدم الثقة هذه.

الخطوة 5: إجراء الترا‌جع (إستعادة ثقة CA)

لعكس تكوين عدم الثقة واستعادة ثقة CA الافتراضية عبر أي إصدار من Cisco IOS XE، حدد دليل قائمة المنع النشطة ($d) بشكل ديناميكي، وقم بإزالة ملفات الشهادات الأربعة التي تمت إضافتها بواسطة هذه الإجراء (بما في ذلك جذر خدمات Comodo AAA)، وأعد إنشاء مخزن الثقة:

<#root>

```
! Escalate to root user inside GuestShell:
[guestshell@guestshell ~]$
```

```
sudo -s
```

```
d=/etc/pki/ca-trust/source/blocklist
[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist

! Remove only the four certificate files added during remediation:
rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" \
"$d/emSign_ECC_Root_CA_-_C3.pem" "$d/emSign_Root_CA_-_C1.pem"

! Rebuild the system CA trust store:
update-ca-trust extract
```

تحقق من عدم إحتواء دليل قائمة الحظر على الملفات التي تمت إزالتها:

<#root>

```
[root@guestshell ~]#
```

```
ls -l "$d"/
```

```
total 0
```

طاق نإلى عاجرإ مت دق ةداهشلا سمخلا نأ نم قحتلا :قدصملا عجرملا ةقث ةداعتسإ دكيأت
ةيلمعلا هذه ءارجإ نم ققحتلا ةوطخلا 3) تاداخلإا عيمج) ليغشت ةداعإ قيرط نع ةطشنلا هاوه قوثوملا طبرلا
:(ةقثلا نع غلبت

<#root>

[root@guestshell ~]#

trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign|AAA'

trust: anchor
trust: anchor
trust: anchor
trust: anchor
trust: anchor

مثال محضر التنفيذ من نهاية إلى نهاية

يوضح النص جلسة تدقيق ومعالجة والتحقق ل GuestShell نجاحة وكاملة على جهاز Cisco IOS XE:

<#root>

Router#

guestshell run bash

[guestshell@guestshell ~]$ sudo -s
bash-4.4#

d=/etc/pki/ca-trust/source/blocklist

bash-4.4#

[-d "$d"] || d=/etc/pki/ca-trust/source/blacklist

bash-4.4#

mkdir -p "$d"

bash-4.4#

trust extract --overwrite --format=pem-bundle \ > --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-

bash-4.4#

```
trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=Comodo%20AAA%20Services%20ro
                                                                                                bash-4.4#
trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-
                                                                                                bash-4.4#
trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20Root%20CA%20-%20C1;
                                                                                                bash-4.4#
                                                                                    update-ca-trust extract
                                                                                                bash-4.4#
                        trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign|AAA'
                                                                                  label: emSign ECC Root CA - G3
                                                                                               trust: blacklisted
                                                                                             category: authority
                                                                                                             --
                                                                                 label: AAA Certificate Services
                                                                                               trust: blacklisted
                                                                                             category: authority
                                                                                                             --
                                                                                  label: emSign ECC Root CA - C3
                                                                                               trust: blacklisted
                                                                                             category: authority
                                                                                                             --
                                                                                      label: emSign Root CA - C1
                                                                                               trust: blacklisted
                                                                                             category: authority
                                                                                                             --
                                                                                      label: emSign Root CA - G1
                                                                                                     trust: anchor
                                                                                             category: authority
                                                                                                bash-4.4#
                                                                                    cat /etc/redhat-release
                                                                                    CentOS Stream release 8
                                                                                                bash-4.4#
                                                                          d=/etc/pki/ca-trust/source/blocklist
                                                                                                bash-4.4#
                                                                  [ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist
```

```
                                                                                bash-4.4#

rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" \ >       "$d/emSign_ECC_Root_C

                                                                                bash-4.4#
                                                                                bash-4.4#

                                                                    update-ca-trust extract

                                                                                bash-4.4#

                                                                    ls -l "$d"/

                                                                        total 0
```

مصفوفة ملخص الأوامر

أمر C	البيئة / الوضع
	EXEC في الامتيازات Cisco IOS XE
	EXEC في الامتيازات Cisco IOS XE
	EXEC في الامتيازات Cisco IOS XE
	GuestShell user Shell
d=/etc/	GuestShell root shell

GuestShell root shell	
GuestShell root shell	
GuestShell root shell	
EXEC ذي الامتيازات Cisco IOS XE	
GuestShell root shell	`rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" "$d/emSign_ECC_Root`

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).