Cisco IOS XE und GuestShell CA Trust Magic - Leitfaden zum Misstrauen

Inhalt

Zweck

Dieses Dokument bietet Anleitungen für Cisco IOS® XE bei der Reaktion auf Misstrauen in Notfällen gegenüber den Mudhra Root and Intermediate Certificate Authorities.

Verwenden Sie diesen Leitfaden, um die Zertifizierungsstellen-Vertrauenswürdigkeit für Dienste zu prüfen und zu verwalten, deren Konfiguration die betroffenen Hierarchien zulässt. Die Anwendbarkeit des Produkts und die erforderlichen Korrekturmaßnahmen sind im Cisco Informationsblatt definiert. Überprüfen Sie die Auswirkungen auf Support und Service für Ihre Cisco IOS XE-Version, bevor Sie die Vertrauensstellung ändern.

Informationen von Cisco: cisco-sa-emudhra-info-ScS22A1r

Betroffene Zertifikate der Mudhra-Zertifizierungsstelle: Original und quersigniert

Bestand am 29. Oktober 2026 überprüft. Acht von eMudhra ausgegebene CA-Schlüssel sind betroffen: sechs für TLS und zwei für Codesignatur. Jeder Schlüssel wird in einem von emSign ausgestellten CA-Zertifikat und einem von Sectigo kreuzsignierten CA-Zertifikat angezeigt. Das Verzeichnis enthält daher 16 Zertifikate: 12 TLS- und 4 Codesignaturzertifikate.

Jedes Original-/Kreuzsignaturpaar hat denselben Betreff und öffentlichen Schlüssel, aber einen anderen Aussteller, eine andere Seriennummer und einen SHA-256-Zertifikat-Fingerabdruck. Die beiden Formulare stellen alternative Zertifizierungswege bereit und müssen beide in eine Prüfung eingebunden werden.

A. Aussteller und betroffenes Zertifikatinventar

Emittent A — Ursprüngliche TLS-Zertifikate: CN=emSign Root TLS CA - G3, O=Mudhra Technologies Limited, C=IN.

Aussteller B — Ursprüngliche Codesignaturzertifikate: CN=emSign Root CS CA - G3, O=Mudhra Technologies Limited, C=IN.

Emittent C — Alle kreuzsignierten Zertifikate: CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB (Sectigo).

G3B-Patienten: O=Mudhra BV, C=NL. Probanden des G3C: O=Mudhra Inc, C=USA. Jede Variantenzelle listet ihren Ausstellerbezug, den hexadezimalen seriellen und den SHA-256-Fingerabdruck (zwei Zeilen) auf. Der Wert für "Leading Zero Padding" ändert keinen seriellen Wert.

Betroffene ausstellende Zertifizierungsstelle (CN)	Ursprüngliches Zertifikat Aussteller / Seriell (hex) / SHA-256	Sectigo-Zertifikat mit Kreuzsignatur Aussteller / Seriell (hex) / SHA-256
1. EM DV TLS CA - G3B TLS	Emittent A A4AE678F23362B4C0E460B772F214 42C4ACCD12C4F59597925E1A08A7A901 02608543809308D50EC427E118BA1493	Emittent C A024FDF4BA665C785CE4A020483858 45A883F349AEDFD5F3A649B5498FFB 1712BA8B448F3F2A91DBC5A766FCDI
2. EM OV TLS CA - G3B TLS	Emittent A 6CADA367FB1C100088120EA202D568 98B896625C0C230ADEEC3EB2CF6AAD50 01ECF9156A68644E82374CE5833BC25B	Emittent C E94223BDE92F914E5AB9ACABFDAC3 5F1DED4DD590AF74631290CF073B12 2AC6A1FA479778A0BD43579BD83269
3. EM EV TLS CA - G3B TLS	Emittent A C7C41EFE92D825F05EAE841A4A82C1 E7568FE6E12331F4FD7DE61DA4C7559D 0F8EB192A218D4741A3BA75184333838	Emittent C D8F8685E4F2BD9D82402A85A1C1EB7 579480AEA166290BD3C643589E795F D0E54E86505D180F1DFF99EFD31995
4. EM DV TLS CA - G3C TLS	Emittent A 588B2E3C2B8CDA13E1A1209254321 0164D7CEAE5BB909C272AF151FF44B11 77AE9B47D9424B94F1D9558C30934D19	Emittent C 91F347F1A5B7D39962B95E0EE4E299 62B7F9868263F72F6911FC78CEAF72 979158B7368BF648683BB2AA39B02E

Betroffene ausstellende Zertifizierungsstelle (CN)	Ursprüngliches Zertifikat Aussteller / Seriell (hex) / SHA-256	Sectigo-Zertifikat mit Kreuzsignatur Aussteller / Seriell (hex) / SHA-256
5. EM OV TLS CA - G3C TLS	Emittent A 296926C227A3A1526392B19482A504 CB6E15165AC802E9B3F993F16C25D41F 4E81C21EBDE71AE1B012AC00BF9C7C3F	Emittent C 8D5A4811939EF447D77111CDD9849A 7485B51C0ED192878FA1D2F948FB52 E1842CC5086C4B67F7BE5B2039DE94
6. EM EV TLS CA - G3C TLS	Emittent A 8009928A64107601AF05FA2F19F109 432EC25F0D28DE9006D97BF752F17BBB 2CD41F669933FCB072D9A1148D0261F3	Emittent C 05F078752DECE7A1BB8595D3031671 FD9D5C2DBBD4995AB69B8D50C439D 7B00529199C2FD01B2174EB58F0702
7. EM OV CS CA - G3B Codesignatur	Emittent B 7818933F8F85B4619A2B35FBA83D0A 9E39DE2881273ACC225A149C72BA3E0F 51424963669AB633EE1DC7DF5DB067B4	Emittent C 41E32B73AC185D6CE0D7480BACF84 A496E23AC0CAB8155FC9B117B97EA 8EFCBB9041AEC8804D5A308D2D01C
8. EM OV CS CA - G3C Codesignatur	Emittent B 544B7F922C31AE220A4A922916F6E6 4B2460A466F95FD40113BCDCCA2CEB29 B3B093921DE45474DA7DF48874C630B1	Emittent C D6A5EF613B390F32EF9CDF349F7728 84112972B8E59D14560AE7E7119654 4AD119990CF3722BFC1E3B91615E1F

B. Zertifizierungspfade zur Unterscheidung

Ursprünglicher TLS-Pfad

```
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
```

Ursprünglicher Code-Signierungspfad (Root CS-vertrauenswürdig direkt)

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

Sectigo-Pfad mit kreuzten Vorzeichen (TLS und Codesignatur)

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

Ein TLS-Pfad kann auch an der emSign-Stamm-TLS-CA - G3 enden, wenn diese CA direkt vertrauenswürdig ist. Die Diagramme zeigen relevante Emittentenbeziehungen. Der akzeptierte Pfad hängt von den Vertrauensankern und der Validierungsrichtlinie des konsumierenden Diensts ab.

Die im Beispiel gezeigten übergeordneten/Stammzertifizierungsstellen bieten Kettenkontext und werden nicht zu den acht kompromittierten Ausgabeschlüsseln gezählt. Die Entscheidung, ein übergeordnetes Element bzw. einen Root zu entfernen oder diesem zu misstrauen, unterscheidet sich von der Identifizierung eines kompromittierten Zwischenschlüssels.

Verwenden Sie zur Identifizierung den Zertifikatausssteller und die Seriennummer zusammen mit dem SHA-256-Fingerabdruck. Ein Subjektname allein reicht nicht aus. Ein Zertifikat-Fingerabdruck identifiziert eine Zertifikatvariante. Ein SPKI SHA-256-Hash identifiziert den öffentlichen Schlüssel, der von seinen ursprünglichen und seinen kreuzsignierten Formularen gemeinsam verwendet wird. Wenn Sie nur eine zwischengespeicherte Zwischenstation entfernen, wird diese von einem Peer nicht durch einen verbleibenden vertrauenswürdigen Pfad dargestellt.

Quellen und Prüfdatum

Die Zertifikatskennungen wurden am 29. Oktober 2026 anhand der öffentlichen Incident-Anhänge überprüft. Jedes Original-/Kreuzsignaturpaar enthält denselben öffentlichen Schlüssel. Live-Informationen von Cisco zur Anwendbarkeit des Produkts und zum Status der Problembehebung

Informationen von Cisco: cisco-sa-emudhra-info-ScS22A1r

Mozilla-Ereignisprotokoll: Mudhra Intermediate Key Compromise (2083449)

Ursprünglicher Anhang mit Zertifizierungsstellenzertifikat (9664066)

AAA-Zertifikatanhang mit Kreuzsignatur (9664067)

Apfel: ursprüngliche und kreuzsignierte TLS-Zertifikatpfade und Fingerprints

Seit dem 31. Oktober 2026 gehört emSign Root CA - G1 nicht zu den kompromittierten CAs, die in diesem Leitfaden aufgeführt sind. Das fortgesetzte Vertrauen unterliegt weiterhin den Richtlinien Ihres Unternehmens und den nachfolgenden Aktualisierungen der Beratung.

Verwaltung der Zertifikatvertrauensstellung mit Cisco IOS XE

Konfigurierte PKI-Vertrauenspunkte enthalten Zertifizierungsstellen-/Identitätszertifikate und Validierungsrichtlinien. Der PKI-Vertrauenspool enthält integrierte und heruntergeladene Zertifizierungsstellenzertifikate für Dienste, die ihn verwenden. Ermittlung der Vertrauensquelle und der Vertrauensrichtlinie, die von den jeweiligen Diensten verwendet werden; Durch das Ändern des Trustpools werden separat konfigurierte Trustpoints nicht ersetzt.

1. Audit und Vorbereitung

Überprüfen Sie die Softwareversion, die Gerätezeit und die installierten Zertifikate:

<#root>

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

Vergleichen Sie den vollständigen Zertifikataussteller und die hexadezimale Seriennummer mit dem Bestand, wobei Sie den Betreff als unterstützenden Kontext verwenden. Wenn Cisco IOS XE nur MD5- und SHA1-Fingerabdrücke anzeigt, kann der SHA-256-Fingerabdruck in dieser Ausgabe nicht direkt verglichen werden. Sie wird zur Überprüfung von Zertifikatsdateien außerhalb des Geräts bereitgestellt. Die Anfangsauffüllung 00 in Seriennummern kann abweichen. Bei der Suche nach Anbieternamen werden nur Kandidaten identifiziert. Notieren Sie die Dienste, die von den einzelnen Vertrauenspunkten abhängen, und überprüfen Sie sowohl den ursprünglichen als auch den kreuzsignierten Pfad, einschließlich der direkt vertrauenswürdigen Intermediate.

Beispiele: Stammzertifizierungsstelle und betroffene Sub-Zertifizierungsstelle

Kurze Beispiele aus dem ausführlichen Zertifikat werden angezeigt. andere Felder werden ausgelassen. Vergleichen Sie Betreff, Aussteller und Seriennummer.

Beispiel für Stamm-CA: emSign ECC-Stammzertifizierungsstelle - G3

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

Beispiel für betroffene SubCA: ezeichen-ausgestelltes Originalzertifikat

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

Beispiel für betroffene SubCA: Sectigo-Zertifikat mit Kreuzsignatur

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

Beide SubCA-Formulare haben denselben Betreff, aber unterschiedliche Emittenten und Serien. Ordnen Sie den vollständigen Aussteller und die Seriennummer dem Inventar zu. führende 00 Polsterung kann abweichen. Notieren Sie die zugeordneten Vertrauenspunkte, um den besitzenden Vertrauenspunkt oder Pool zu ermitteln. Der dargestellte Stamm ist der Kettenkontext. es handelt sich nicht um einen der acht kompromittierten Ausgabeschlüssel.

Halten Sie eine Wiederherstellungszugriffsmethode und ein genehmigtes Ersatzpaket bereit.

Verwenden Sie ggf. das genehmigte Zertifikat/den genehmigten Schlüssel als Backup. Erstellen Sie eine Sicherungskopie der Konfiguration. Diese Kopie ist keine Sicherung mit privatem Schlüssel:

<#root>

```
copy running-config <BACKUP-CONFIG-URL>
```

Ersetzen Sie Platzhalter für spitze Klammern durch genehmigte gerätespezifische Werte. Verwenden Sie ein Dateisystem, das durch Dateisysteme angezeigt wird, wie z. B. flash: oder bootflash:.

2. Vertrauenswürdige Pfade überprüfen

Direkt vertrauenswürdige betroffene SubCAs entfernen

Entfernen Sie direkt vertrauenswürdige betroffene SubCAs von Trustpoints und heruntergeladenen Trustpool-Paketen. Verlassen Sie sich nicht auf die Sperreinstellungen, um die direkte Vertrauenswürdigkeit in einer kompromittierten Zertifizierungsstelle außer Kraft zu setzen.

Optionale Entfernung der Stammzertifizierungsstelle

Das Entfernen der Root-Zertifizierungsstelle ist eine optionale Empfehlung für zusätzlichen Schutz. Ein erforderlicher Stamm kann vertrauenswürdig bleiben, wenn die eigentlichen CRL/OCSP-Serviceprüfungen den aktuellen Status abrufen, die betroffene SubCA unter einem vertrauenswürdigen übergeordneten Element auswerten, betroffene Original-, Cross-Signed- und anwendbare längere Ketten zurückweisen und eine Fail-Validierung durchführen, wenn keine der konfigurierten Methoden einen nutzbaren Status bereitstellt. Unter diesen verifizierten Bedingungen schützt die Widerrufskontrolle gegen die identifizierten kompromittierten Emittenten, ohne die Wurzel zu löschen.

Entfernen Sie ggf. unnötige Stamm-/Vertrauensanker, um die Abhängigkeit von Sperrdiensten zu reduzieren. Zuerst die Service-Abhängigkeiten bewerten: Durch das Entfernen von AAA-Zertifikatdiensten können unabhängige legitime Ketten unterbrochen werden. Decken Sie sowohl Medhra- als auch AAA-Pfade ab. Durch das Löschen einer zwischengespeicherten SubCA wird eine vom Peer bereitgestellte Kopie nicht durch ein verbleibendes vertrauenswürdiges übergeordnetes Element blockiert.

Ausgewählten Vertrauenspunkt entfernen

Für einen vom Administrator konfigurierten Vertrauenspunkt, der zum Entfernen ausgewählt wurde:

<#root>

```
configure terminal no crypto pki trustpoint <TRUSTPOINT-NAME> end
```

Überprüfen Sie die Bestätigung, bevor Sie sie akzeptieren. Durch Entfernen des Vertrauenspunkts werden die zugehörigen Zertifikate gelöscht. Wenn eine Geräteidentität ersetzt werden muss, holen Sie sich ein Ersatzzertifikat, das mit dem Geräteschlüssel übereinstimmt, und aktualisieren Sie die Dienstbindung mithilfe des Verfahrens zur Registrierung des Diensts. Durch die Installation eines neuen Zertifizierungsstellenzertifikats allein wird die Geräteidentität nicht ersetzt.

Verwenden Sie für heruntergeladene Trustpool-Einträge das Verfahren zum Austausch von Paketen. Integrierte Anker oder Anker mit integriertem oder verwaltetem Funktionsumfang erfordern eine unterstützte Produktaktualisierung oder Beratung durch das Cisco TAC.

3. Aktualisieren Sie ggf. den heruntergeladenen Trustpool.

Gehen Sie wie folgt vor, wenn ein heruntergeladenes Paket ersetzt werden muss. Ein erforderliches übergeordnetes Element bzw. eine erforderliche Root kann unter den in Schritt 2 beschriebenen und geprüften Sperrbedingungen vertrauenswürdig bleiben.

3.1 Überprüfen Sie, ob ein heruntergeladenes Paket installiert und verwendet wird.

<#root>

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

Suchen Sie nach Cabundle-Einträgen unter dem Crypto-PKI-Zertifikatpool und den CA-Einträgen, die als Trustpool gekennzeichnet sind: Heruntergeladen. Die Paketdateinamen können sich von ios.p7b oder ios_core.p7b unterscheiden. Eine gespeicherte Datei oder eine konfigurierte Aktualisierungs-URL allein beweist nicht, dass die Zertifikate von einem Dienst installiert oder verwendet werden. Bestätigen Sie, dass der Service den Vertrauenspool verwendet, und vergleichen Sie seine Zertifizierungsstellendatensätze mit dem betroffenen Bestand. Wenn keine heruntergeladenen CAs installiert sind, überspringen Sie die Bereinigung und den Austausch. andere Vertrauensquellen zu analysieren.

3.2 Bereinigen Sie den heruntergeladenen Trustpool.

Halten Sie vor der Bereinigung den Wiederherstellungszugriff und ein genehmigtes Wiederherstellungspaket verfügbar. Das anschließende Herunterladen kann fehlschlagen, wenn die Übertragung von der entfernten Vertrauensstellung abhängt. Planung der Unterbrechung abhängiger Dienste

<#root>

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

```
show crypto pki trustpool verbose
```

Bestätigen Sie, dass heruntergeladene CA-Datensätze nicht mehr vorhanden sind. Beim Cleanup werden alle heruntergeladenen Trustpool-Zertifikate und die zugehörigen verwalteten Paketdateien entfernt. integrierte CAs und separate Trustpoints bleiben erhalten. Speichern Sie die Daten erst, wenn die Überprüfung des Ersatzes und der Services erfolgreich abgeschlossen wurde.

3.3 Erhalt und Installation des genehmigten Ersatzpakets

Fordern Sie ein genehmigtes Paket mit Cisco Signatur an. Wählen Sie ios.p7b oder ios_core.p7b für die erforderlichen Dienste aus, und bestätigen Sie, dass die oben angegebenen betroffenen Zertifikate und unerwünschten Vertrauensanker ausgeschlossen werden. Die am 31. Oktober 2026 überprüften Legacy-Pakete enthalten die emSign-Stammzertifizierungsstelle - G1 in ios.p7b, jedoch weder Medhra noch AAA-Zertifizierungsstellen für Zertifikatsdienste in ios_core.p7b. Der Core verfügt über eine kleinere Vertrauensgruppe: Überprüfen Sie vor dem Switching die Service-Abhängigkeiten, und überprüfen Sie den Inhalt des Pakets, das Sie installieren. Sie können sie außerhalb des verwalteten Trustpool-Speichers mithilfe eines genehmigten HTTPS- oder SCP-Transfers bereitstellen.

Cisco CA-Komplettpaket: ios.p7b

Cisco Core CA-Paket: ios_core.p7b

<#root>

```
show file systems copy <APPROVED-BUNDLE-SOURCE-URL> <STAGED-BUNDLE-URL> configure terminal crypto pki tr
```

Die bereitgestellte URL kann z. B. flash:approved-ios.p7b lauten. Wenn der Import fehlschlägt, stellen Sie ein genehmigtes Paket vor dem Speichern wieder her. Überprüfen Sie die beabsichtigten CAs und erforderlichen Verbindungen. Die Bereinigung ist keine Zertifikatdenyliste: Bestätigung der verbleibenden Vertrauenspunkte, integrierten Zertifizierungsstellen und alternativen Pfade, die betroffene Ketten ablehnen, durch erzwungenen Widerruf oder Entfernen von Vertrauenspfaden.

4. Validierungs- und Aktualisierungsrichtlinie konfigurieren

Bevor Sie Änderungen vornehmen, notieren Sie sich die vorhandene Trustpool-Richtlinie, betroffene Trustpoint-Richtlinien, Zertifikatzuordnungsbindungen und Aktualisieren-URLs, damit diese bei Bedarf wiederhergestellt werden können.

Für relevante konfigurierte Vertrauenspunkte:

<#root>

```
configure terminal crypto pki trustpoint <VALIDATION-TRUSTPOINT> revocation-check crl ocsp exit end
```

Für Services, die die Trustpool-Richtlinie verwenden:

<#root>

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

Stellen Sie sicher, dass die angezeigte Trustpool-Richtlinie die Validierung an den Root fortsetzt und crl ocsp auflistet. Das Gerät testet zuerst die Sperrliste und versucht dann den OCSP, wenn der Sperrlistenabruf nicht verfügbar ist. Ein gesperrtes Ergebnis schlägt bei der Validierung fehl, wenn das betroffene Zertifikat ausgewertet wird. Fügen Sie keine hinzu, wenn eine erfolgreiche Sperrung erforderlich ist.

Überprüfen Sie die korrekte Zeit, die erreichbaren, von der Zertifizierungsstelle veröffentlichten Statusendpunkte, die akzeptierten Antwortformate und das Fehlen anwendbarer Ausnahmen zum Überspringen der Sperrung. Der Status der betroffenen Sub-CAs muss unter einem vertrauenswürdigen übergeordneten Element ausgewertet werden. Die direkte Vertrauenswürdigkeit in dieser SubCA kann die Validierung beenden, bevor die übergeordnete CA überprüft wird. Überprüfen Sie, ob der tatsächliche Service den verfügbaren, aktuellen Status

erhält und die betroffenen Ketten zurückweist. Wenn das Zugriffs- und Ablehnungsverhalten des Status-Servers nicht überprüft werden kann, behandeln Sie die Konfiguration nicht als bestätigten Schutz. Entfernen Sie die relevanten Vertrauenspfade, wenn dies nach Ihrem Eindämmungsplan erforderlich ist. Fügen Sie keine hinzu, um den Status "Nicht verfügbar" zu umgehen.

Aktualisierung der zwischengespeicherten Zertifikatsperrlisten vor Überprüfung des Schutzes

Eine bereits im lokalen Cache/in der lokalen Datenbank vorhandene, verwendbare Zertifikatsperrliste kann auch nach Veröffentlichung einer neueren Zertifikatsperrliste durch die Zertifizierungsstelle wiederverwendet werden. Überprüfen Sie die Erreichbarkeit des Status-Servers, und löschen Sie dann die alten Zertifikatsperrlisten, bevor Sie den Schutz validieren:

<#root>

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

Mit dem Befehl clear werden lokale Zertifikatsperrlisten für alle Vertrauenspunkte entfernt. Es lädt selbst keine Ersatzteile herunter. Bestätigen Sie, dass die alten Einträge entfernt sind, und initiieren Sie dann eine neue Verbindungs- oder Zertifikatsüberprüfung im betroffenen Dienst. Führen Sie show crypto pki crls erneut aus, und überprüfen Sie alle relevanten Aussteller, LastUpdate, NextUpdate und Verteilungspunkte mit den aktuellen Veröffentlichungen der Zertifizierungsstellen. Berücksichtigen Sie die CRL der übergeordneten Emittenten, die die betroffene SubCA abdeckt, und nicht nur die CRL des ID-Zertifikatausstellers. Bestätigt, dass betroffene Ketten abgelehnt wurden. Das Löschen kann sich vorübergehend auf neue Verbindungen auswirken, während Statusdaten abgerufen werden. die Fail-Closed-Validierung aufrecht zu erhalten.

Überprüfen der Paketaktualisierungsquelle

Konfigurieren Sie für angeschlossene Geräte optional die genehmigte ablaufgesteuerte Paketaktualisierungsquelle:

<#root>

configure terminal crypto pki trustpool policy cabundle url <APPROVED-REFRESH-BUNDLE-URL> exit end show

Überprüfen Sie alle konfigurierten Paketquellen. Eine ablaufgesteuerte Aktualisierung ersetzt keine sofortige Sicherheitsaktualisierung und darf keinen unerwünschten Vertrauenspfad wiederherstellen.

Optionaler Zertifikatzuordnungsfilter: Abdeckung und Begrenzung

Eine Cisco IOS XE-Zertifikatszuordnung (cert-map) entspricht Zertifikatattributen, z. B. dem Namen des Ausstellers. Als zusätzliche Maßnahme kann der Filter dazu beitragen, ID-Zertifikate (Leaf-Zertifikate) abzulehnen, die direkt von den acht aufgeführten Zertifizierungsstellen ausgestellt wurden. Überprüfen Sie vor der Anwendung die Richtlinie für vorhandene Übereinstimmungszertifikate für Trustpoints.

Das Verhalten wurde am 29. Oktober 2026 unter Verwendung von Laboridentitäten unter EM DV TLS CA - G3B auf experimentellen Laborgeräten getestet. Bei der PKI-Peer-Zertifikatvalidierung hat der Filter eine direkt ausgestellte Identität zurückgewiesen, jedoch keine Identität blockiert, die über eine zusätzliche untergeordnete SubCA ausgegeben wurde. ein nicht börsennotierter legitimer Emittent bestanden hat. Die verhaltensbasierte Abdeckung verwendete einen betroffenen Aussteller, wobei die Sperrung nur für temporäre Lab-Vertrauenspunkte deaktiviert wurde, um den Filter zu isolieren. Anwendungs-Handshakes und andere Versionen wurden mit diesem Filter nicht validiert. den eigentlichen Dienst testen, bevor er sich darauf verlässt.

<#root>

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

Hier bedeutet nc "enthält nicht". Achten Sie darauf, dass alle acht Bedingungen für einen negativen Namen des Emittenten in der gleichen Zeile, Sequenz 10, beibehalten werden: Alle müssen übereinstimmen, damit das Zertifikat diesen Filter übergeben kann. Ein direkter Aussteller, der mit einem aufgelisteten Namen übereinstimmt, schlägt mit dem Filter fehl.

In Cisco IOS XE können normalisierte Einträge angezeigt werden, z. B. Issuer-Name nc cn = em dv tls ca - g3b. Dieses Kleinbuchstaben- und Abstandsformat wurde im Verhaltenstest verwendet. Bestätigen Sie die Zuordnung und deren Bindung an den vom Dienst tatsächlich verwendeten Vertrauenspunkt:

<#root>

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

Der Filter stellt keine kettenweite CA-Denyliste bereit. Beispiele:

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

Der ID-Zertifikataussteller ist die neue untergeordnete SubCA, daher identifiziert der Ausstellername-Filter die betroffene CA nicht weiter oben in der Kette. Andere Prüfungen, einschließlich CA-Einschränkungen und Widerruf, gelten weiterhin. Verwenden Sie diesen Filter nur als zusätzlichen Schutz zusammen mit der Sperrvalidierung und den optionalen Verfahren zum Entfernen von Roots in diesem Leitfaden. Direkt ausgestellte, Child-SubCA- und legitime Zertifikate mit dem eigentlichen Dienst testen.

Zurücksetzen von Schritt 4

Stellen Sie die aufgezeichneten Sperrmethoden, Kettenvalidierungseinstellungen und Zertifikatzuordnungsbindungen wieder her. Entfernen Sie die von diesem Verfahren hinzugefügten Aktualisierungs-URLs, und stellen Sie alle zuvor geänderten URLs wieder her. In diesem Beispiel werden nur der hinzugefügte Aktualisierungs-URL und die Filterbindung entfernt. Die anderen Richtlinieneinstellungen werden nicht wiederhergestellt:

<#root>

```
configure terminal crypto pki trustpool policy no cabundle url <ADDED-REFRESH-BUNDLE-URL> exit
```

```
crypto pki trustpoint <VALIDATION-TRUSTPOINT> no match certificate EMSIGN-ISSUER-FILTER exit end
```

Führen Sie diese Deinstallationen nur dann aus, wenn die URL und die Bindung durch dieses Verfahren hinzugefügt wurden. Wenn eine vorherige Zertifikatzuordnungsbindung ersetzt wurde, stellen Sie sie wieder her. Entfernen Sie eine neu erstellte Zuordnung erst, nachdem Sie bestätigt haben, dass keine andere Konfiguration auf sie verweist.

Verwenden Sie keine crypto pki trustpool-Richtlinie nur, wenn das Zurücksetzen auf die Standardwerte das beabsichtigte, genehmigte Ergebnis ist. Durch dieses weit reichende Zurücksetzen werden konfigurierte Aktualisierungs-URLs gelöscht und die Sperrprüfung auf "none" zurückgesetzt. Die vorherige benutzerdefinierte Richtlinie wird nicht wiederhergestellt. Beim Richtlinien-Rollback werden gelöschte Zertifikate nicht wiederhergestellt, das installierte

Paket zurückgesetzt oder gelöschte Zertifikatsperrlisten wiederhergestellt. Überprüfen Sie vor dem Speichern erneut die erforderlichen Services und die Ablehnung der betroffenen Kette.

5. Überprüfen Sie den Schutz und speichern

- Vergewissern Sie sich, dass die betroffenen ursprünglichen und kreuzsignierten Ketten abgelehnt werden, einschließlich eines vom Peer bereitgestellten Intermediärs. Wenn längere Ketten relevant sind, überprüfen Sie die Ablehnung, wenn die betroffene CA höher in der Kette ist.
- Vergewissern Sie sich, dass die erforderlichen legitimen Verbindungen weiterhin funktionieren und dass die Austausch-Identität an den beabsichtigten Dienst gebunden ist.
- Verhalten überprüfen, wenn Sperrdaten nicht verfügbar sind Bestehende TLS/IPsec-Sitzungen werden nicht automatisch durch eine Richtlinienänderung validiert. Verwenden Sie ggf. das vom Dienst unterstützte Verfahren zur erneuten Verbindung.

Nach erfolgreicher Überprüfung:

<#root>

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

Überprüfen Sie die Persistenz nach dem nächsten geplanten Neuladen und gegebenenfalls auf dem Standby-Gerät. Wenn die Ergebnisse von den erwarteten Vertrauensrichtlinien abweichen, bewahren Sie die Protokolle auf, und wenden Sie sich an das Cisco TAC, bevor Sie die überprüften Vertrauensänderungen in Erwägung ziehen.

Weitere Informationen

Management von Cisco IOS XE PKI-Vertrauenspools

Cisco: Konfigurieren von CA-signierten Zertifikaten mit der Cisco IOS XE PKI

Cisco: Sperrlisten-Zwischenspeicherung und Sperrprüfung

Cisco IOS XE GuestShell CA Trust Guide

Schritt 1: Überwachung des GuestShell-Bereitstellungsstatus des Geräts

Die Behebung ist nur auf Cisco IOS XE-Systemen erforderlich, auf denen GuestShell installiert ist, und zwar im Status "RUNNING" oder "DEPLOYED". Wenn sich GuestShell im DEPLOYED-Zustand befindet, muss sie zunächst mit dem Befehl "guestshell enable" aktiviert werden, bevor Wiederherstellungsbefehle ausgeführt werden. Wenn die Anzeige der App-Hostingliste anzeigt, dass keine App gefunden wurde (GuestShell ist nicht bereitgestellt oder aktiviert), ist für GuestShell keine Aktion erforderlich.

A. GuestShell im BEREITGESTELLTEN Zustand (Aktion erforderlich: Muss zuerst aktiviert werden)

Wenn show app-hosting list GuestShell im Zustand DEPLOYED meldet, ist GuestShell-Containerspeicher vorhanden, der Container wird jedoch beendet. Sie müssen 'guestshell enable' ausführen, bevor Sie bash eingeben (und optional 'guestshell disable', nachdem Sie die Behebung abgeschlossen haben, wenn Sie zu einem angehaltenen Zustand zurückkehren):

<#root>

```
Router#

show app-hosting list

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

B. GuestShell im Status "RUNNING" (Aktion erforderlich: Direkt fortfahren)

Wenn show app-hosting list GuestShell im Status RUNNING anzeigt, wird GuestShell aktiv ausgeführt, und Sie können direkt mit bash fortfahren:

<#root>

```
Router#

show app-hosting list
```

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

B. GuestShell nicht aktiviert/nicht bereitgestellt (keine Aktion erforderlich)

Wenn "show app hosting list" anzeigt, dass keine App gefunden wurde, ist GuestShell nicht auf dem System installiert oder aktiviert, und es ist keine weitere Aktion erforderlich:

<#root>

```
Router#

show app-hosting list

No App found
```

Phase 2: Zugreifen auf GuestShell und Anwenden von CA Misstrauen

Führen Sie diese Befehle an der Eingabeaufforderung für den privilegierten EXEC-Modus von Cisco IOS XE aus ('enable'). Wenn sich GuestShell im DEPLOYED-Zustand befindet, aktivieren Sie es zuerst. Geben Sie dann die Bash-Shell ein, eskalieren Sie zu root, und konfigurieren Sie die CA-Sperrliste mithilfe der dynamischen Ordnerauswahl, um die Kompatibilität aller Cisco IOS XE-Versionen sicherzustellen:

<#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"
```

Verstörende kompromittierte Mudhra-Zertifikate

Führen Sie die Befehle trust extrahieren aus, um jedes kompromittierte eMudhra-Zertifikat direkt in das ca-trust blocklist-Verzeichnis zu extrahieren. Anschließend wird der System-Trust-Speicher neu erstellt:

```
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
```

Schritt 3: Überprüfen von vertrauenswürdigen Zertifikaten in GuestShell

Vergewissern Sie sich, dass die vier extrahierten Zertifikate in der Richtlinie für Misstrauen/Sperrlisten des Systems angezeigt werden und mithilfe des folgenden Verifizierungsbefehls von den aktiven Vertrauensankern ausgeschlossen werden. Mit dem Befehl wird bestätigt, dass die Zertifikate in der Sperrlistenrichtlinie registriert sind.

```
###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
```

Schritt 4: Statuspersistenz und Container-Lebenszyklus

Hinweis zur Containerpersistenz: Diese Änderungen an Zertifikatsvertrauensstellungen bestehen über die Vorgänge "guestshell enable" und "guestshell disable" fort, und das Gerät wird neu gestartet, weil /etc/pki/ca-trust auf dem permanenten Containerspeicher gespeichert ist.

Rückkehr in den BEREITGESTELLTEN Zustand (falls zutreffend): Wenn GuestShell ursprünglich den Status DEPLOYED hatte und nur für die Ausführung dieser Misstrauensprozedur aktiviert wurde, setzen Sie GuestShell auf den Status "Stopped" zurück, indem Sie bash beenden und "guestshell disable" über die IOS-Eingabeaufforderung für privilegierten EXEC-Modus ausführen:

<#root>

```
[root@guestshell ~]#

exit

[guestshell@guestshell ~]$

exit

Router#

guestshell disable
```

Wichtige Überlegungen zum Lebenszyklus: Wenn GuestShell mit 'guestshell destroy' vollständig zerstört wird, wird das Container-Dateisystem entfernt. Wenn GuestShell anschließend erneut

aktiviert wird, wird der Container aus dem Basissystem-Image neu erstellt, und diese Schritte zur Beseitigung von Misstrauen müssen erneut angewendet werden.

Schritt 5: Rollback-Verfahren (Wiederherstellung der CA-Vertrauenswürdigkeit)

Um die Vertrauensstellung umzukehren und die standardmäßige CA-Vertrauensstellung für alle Cisco IOS XE-Versionen wiederherzustellen, wählen Sie das aktive Sperrlistenverzeichnis ($d) dynamisch aus, entfernen Sie die vier Zertifikatsdateien, die durch dieses Verfahren hinzugefügt wurden (einschließlich Comodo AAA Services-Root), und erstellen Sie den Vertrauensspeicher neu:

<#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
```

Vergewissern Sie sich, dass das Sperrlistenverzeichnis die entfernten Dateien nicht mehr enthält:

<#root>

```
[root@guestshell ~]#

ls -l "$d"/

total 0
```

Wiederherstellung der CA-Vertrauensstellung bestätigen: Stellen Sie sicher, dass alle fünf Zertifikate wieder an aktive Vertrauensanker zurückgegeben wurden, indem Sie den Verifizierungsbefehl für Schritt 3 erneut ausführen (alle Einträge melden Vertrauenswürdigkeit: Anker):

<#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
```

Transkriptbeispiel für die End-to-End-Ausführung

Das Protokoll veranschaulicht eine vollständige und erfolgreiche GuestShell-Audit-, Wiederherstellungs- und Verifizierungssitzung auf einem Cisco IOS XE-Gerät:

<#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
```

Befehlsübersicht

Betriebliche Aufgabe	
GuestShell-Status überwachen	`show app-hosting list`
GuestShell aktivieren (falls BEREITGESTELLT)	`guestshell enable`
GuestShell-Bash eingeben	`guestshell run bash`
Zum Stammbenutzer wechseln	`sudo -s`
Blocklistenverzeichnis vorbereiten	`d=/etc/pki/ca-trust/source/blocklist; [ -d "$d" ] || d=/etc/pki/ca-trust/sou`
CAs in Sperrliste extrahieren	`trust extract --overwrite --format=pem-bundle ... (x4 CAs)`
Wiederherstellung des CA Trust Store	`update-ca-trust extract`
Überprüfung der Vertrauensrichtlinie	`trust list --filter=trust-policy --purpose=server-auth`

BEREITGESTELLTEN Zustand wiederherstellen (optional)	`guestshell disable`
Rollback/Wiederherstellung der Vertrauenswürdigkeit	`rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" "$d`

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.