Kompatibilitätsproblem mit der Zertifikatkette des WebEx Calling Survivability Gateway

Inhalt

Problem

Bei der Konfiguration der WebEx-Überlebensfähigkeit für Anrufe und der Aktivierung des Testmodus im Control Hub schlägt die Synchronisierung des Gateways mit WebEx Cloud-Servern fehl. Der Befehl show voice register session zeigt nicht das erwartete Registrierungsverhalten an, und der Control Hub zeigt Synchronisierungsfehler an.

In den Telemetrie-Protokollen wird dieser Fehler bei Synchronisierungsversuchen angezeigt:

```
2026-08-12T19:22:58.745Z - ERROR - Thread-5 (handle_sgw_events) - wxcc_sgw_manager : TELEMETRYLOG : WxC
```

Das Gateway stellt für den konfigurierten Standort keine sichere TLS-Verbindung mit WebEx Cloud her und verhindert so eine ordnungsgemäße Synchronisierung und Registrierung des Survivable Gateways.

Umwelt

- Konfiguration des WebEx Calling Survivable Gateway
- IOS XE-Softwareversion 17.12.6
- GoDaddy TLS-Zertifikate auf dem Gateway installiert
- Zertifikatskette mit GoDaddy TLS Intermediate CA DV - R1v1
- Control Hub-Ausfallsicherheitskonfiguration mit aktiviertem Testmodus

Auflösung

Dieses Problem wurde behoben, indem das Zertifikat durch ein Zertifikat ersetzt wurde, das eine unterstützte Zertifizierungsstellenkette verwendet. Das problematische Zertifikat wurde mit der neueren GoDaddy R1v1-Zertifikatskette erstellt, die von den WebEx Calling-Plattformen nicht unterstützt wird.

Schritt 1: Überprüfung der aktuellen Zertifikatkette

Überprüfen Sie die derzeit auf dem Kabelmodem installierten Zertifikate:

```
device# show crypto pki certificates
```

Die Ausgabe zeigt die problematische Zertifikatskette an:

<#root>

```
Certificate
  Status: Available
  Certificate Serial Number (hex): 00923AC809A58436DD
  Certificate Usage: General Purpose
  Issuer:
```

cn=GoDaddy TLS Intermediate CA DV - R1v1

```
    o=GoDaddy.com
    c=US
  Subject:
    Name: mhtlc-ls-r1.mhtlc.org
```

cn=mhtlc-ls-r1.mhtlc.org

```
  CRL Distribution Points:
    http://crl.godaddy.com/gdr1v1dv_s1-7.crl
  Validity Date:
    start date: 13:43:39 CDT Jun 25 2026
    end   date: 12:43:39 CST Jan 9 2027
  Associated Trustpoints: webex-sgw
  Storage: nvram:GoDaddyTLSIn#36DD.cer
```

Phase 2: Identifizieren von Zertifikatskette-Kompatibilitätsproblemen

Die Zertifikatanalyse ergab, dass das Gateway ein Zertifikat verwendet, das von der GoDaddy TLS Intermediate CA DV - R1v1 signiert wurde. Das Kreuzzertifikat (GoDaddy TLS Root CA - R1) und das Stammzertifikat (Go Daddy Root Certificate Authority - G2) fehlten im Gateway.

WebEx Calling unterstützt nur Zertifikate mit der Stammzertifizierungsstelle "GoDaddy" gemäß offizieller Dokumentation.

- CN=Go Daddy Root Certificate Authority - G2

Schritt 3: Neues Zertifikat mit unterstützter Kette anfordern

Wenden Sie sich an den Zertifikatanbieter (GoDaddy), um das Zertifikat erneut zu schlüsseln und sicherzustellen, dass die unterstützte Zertifikatkette verwendet wird:

- Fordern Sie ein neues Zertifikat für denselben Domänen-FQDN an (mhtlc-ls-r1.mhtlc.org).
- Geben Sie an, dass das Zertifikat die Zertifikatskette GoDaddy G2 (SHA-2) verwenden muss.
- Stellen Sie sicher, dass alle relevanten Zertifikate für eine vollständige Vertrauenskette auf dem SGW-Router installiert sind.

Schritt 4: Neues Zertifikat installieren

Sobald Sie das neue Zertifikat mit der unterstützten G2-Kette erhalten haben, installieren Sie es auf dem Survivability Gateway, und konfigurieren Sie den entsprechenden Vertrauenspunkt für die WebEx-Konnektivität.

Führen Sie diesen Schritt aus, wenn ein öffentlich bekanntes CA-Root-Zertifikat mit Ihrem Cisco IOS XE-Gateway nicht verfügbar ist.

```
crypto pki trustpoint <CA name>
 enrollment terminal
 revocation-check crl
 crypto pki authenticate <CA name>
```

Schritt 5: Auflösung überprüfen

Testen Sie nach der Installation des neuen Zertifikats die Registrierung des Survivable Gateway:

- Überwachen Sie den Synchronisierungsprozess im Control Hub.
- Überprüfen Sie die erfolgreiche Registrierung, indem Sie den Befehl show voice register session ausführen.
- Stellen Sie sicher, dass in den Telemetrieprotokollen keine TLS-Verbindungsfehler mehr angezeigt werden.

Ursache

Die Ursache war die Inkompatibilität der Zertifikatskette zwischen dem Survivability Gateway und den WebEx Calling Cloud Services. Das Gateway wurde mit einem Zertifikat konfiguriert, das von GoDaddy TLS Intermediate CA DV - R1v1 signiert wurde und Teil der neueren GoDaddy R1-Zertifikatskette ist.

WebEx Calling unterstützt nur Zertifikate, die sich an die Go Daddy Root Certificate Authority - G2 anschließen. Die neuere R1v1-Zwischenzertifikatsautorität, die von GoDaddy eingeführt wurde, ist nicht in der Liste der vertrauenswürdigen WebEx Callings-Zertifizierungsstellen enthalten, was zu TLS-Handshake-Fehlern während des Überlebensfähigkeits-Gateway-Synchronisierungsprozesses führt. Darüber hinaus verhinderte das fehlende Stammzertifikat auf dem Gateway eine ordnungsgemäße Validierung der Zertifikatskette, was zu Fehlern beim Aufbau einer sicheren Verbindung beitrug.

Verwandte Inhalte

- Unterstützte Stammzertifizierungsstellen für Anrufe bei Cisco WebEx Audio- und Videoplattformen
- Technischer Support und Downloads von Cisco
- Survivable Site für WebEx Anrufe

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.