Webex Calling Survivability Gateway 인증서 체인 호환성 문제

목차

문제

Control Hub에서 Webex Calling Survivability를 구성하고 테스트 모드를 활성화하면 게이트웨이가 Webex 클라우드 서버와 동기화되지 않습니다. show voice register session 명령은 예상 등록 동작을 표시하지 않으며 Control Hub에 동기화 오류가 표시됩니다.

동기화 시도 중에 텔레메트리 로그에 이 오류가 표시됩니다.

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

게이트웨이가 구성된 위치에 대해 Webex Cloud와의 보안 TLS 연결을 설정하지 못해 존속성 게이트웨이의 올바른 동기화 및 등록을 방해합니다.

환경

- Webex Calling Survivability Gateway 컨피그레이션
- IOS XE Software 버전 17.12.6
- 게이트웨이에 설치된 GoDaddy TLS 인증서
- GoDaddy TLS Intermediate CA DV를 사용하는 인증서 체인 - R1v1
- 테스트 모드가 활성화된 제어 허브 존속성 컨피그레이션

해결

이 문제는 지원되는 인증 기관 체인을 사용하는 인증서로 대체하여 해결되었습니다. 문제가 있는 인증서가 Webex Calling 플랫폼에서 지원하지 않는 최신 GoDaddy R1v1 인증서 체인을 사용하고 있었습니다.

1단계: 현재 인증서 체인 확인

게이트웨이에 현재 설치된 인증서를 확인합니다.

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

출력에 문제가 있는 인증서 체인이 표시됩니다.

<#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
```

2단계: 인증서 체인 호환성 문제 식별

인증서 분석 결과 게이트웨이가 GoDaddy TLS Intermediate CA DV - R1v1에서 서명한 인증서를 사용하고 있음이 확인되었습니다. 교차 인증서(GoDaddy TLS Root CA - R1)와 루트 인증서(Go Daddy Root Certificate Authority - G2)가 게이트웨이에서 누락되었습니다.

Webex Calling은 공식 문서마다 "GoDaddy" 루트 인증 기관이 있는 인증서만 지원합니다.

- CN=Go Daddy Root Certificate Authority - G2

3단계: 지원되는 체인으로 새 인증서 요청

인증서 키 재설정을 위해 인증서 공급자(GoDaddy)에 문의하여 지원되는 인증서 체인을 사용하는지 확인합니다.

- 동일한 도메인 FQDN(mhtlc-ls-r1.mhtlc.org)에 대해 새 인증서를 요청합니다.
- 인증서가 GoDaddy G2(SHA-2) 인증서 체인을 사용해야 함을 지정합니다.
- 완전한 신뢰 체인에 대한 모든 관련 인증서가 SGW 라우터에 설치되어 있는지 확인합니다.

4단계: 새 인증서 설치

지원되는 G2 체인의 새 인증서를 가져오면 존속성 게이트웨이에 설치하고 Webex 연결에 적합한 신뢰 지점을 구성합니다.

Cisco IOS XE 게이트웨이에서 공개적으로 알려진 CA 루트 인증서를 사용할 수 없는 경우 이 단계를 수행합니다.

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

5단계: 해결 확인

새 인증서를 설치한 후 존속성 게이트웨이 등록을 테스트합니다.

- Control Hub에서 동기화 프로세스를 모니터링합니다.
- show voice register session 명령을 실행하여 성공적인 등록을 확인합니다.
- 텔레메트리 로그에 더 이상 TLS 연결 오류가 표시되지 않는지 확인합니다.

원인

근본 원인은 존속성 게이트웨이와 Webex Calling 클라우드 서비스 간의 인증서 체인 비호환성이었습니다. 게이트웨이가 GoDaddy TLS Intermediate CA DV - R1v1에서 서명한 인증서로 구성되었습니다. 이 인증서는 최신 GoDaddy R1 인증서 체인의 일부입니다.

Webex Calling은 Go Daddy Root Certificate Authority - G2로 연결되는 인증서만 지원합니다. GoDaddy에서 도입한 최신 R1v1 중간 인증 기관은 Webex Calling 트러스트된 인증 기관 목록에 포함되어 있지 않으므로 존속성 게이트웨이 동기화 프로세스 중에 TLS 핸드셰이크 오류가 발생합니다. 또한 게이트웨이의 루트 인증서가 누락되어 올바른 인증서 체인 유효성 검사를 할 수 없으므로 보안 연결 설정에 장애가 발생했습니다.

관련 콘텐츠

- Cisco Webex 오디오 및 비디오 플랫폼 통화에 지원되는 루트 인증 기관
- Cisco 기술 지원 및 다운로드
- Webex 통화를 위한 사이트 존속성

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.