2020년 1월 1일 IOS 자체 서명 인증서 만료

목차

소개

참고: 이 문서에는 FN40789의 내용과 추가적인 컨텍스트, 예제, 업데이트 및 Q&A가 포함되어 있습니다.

2020년 1월 1일(UTC) 00:00에 IOS/IOS-XE 시스템에서 생성된 모든 SSC(Self-Signed Certificates)는 SSC가 생성될 때 시스템이 고정 버전의 IOS/IOS-XE를 실행하지 않는 한 만료됩니다. 이 시간이 지나면 고정되지 않은 IOS 시스템은 새 SSC를 생성할 수 없습니다. 이러한 자체 서명 인증서를 사용하여 보안 연결을 설정하거나 종료하는 모든 서비스는 인증서가 만료된 후에 작동하지 않을 수 있습니다.

이 문제는 Cisco IOS 또는 Cisco IOS XE 디바이스에서 생성되어 디바이스의 서비스에 적용된 자체

서명 인증서만 영향을 미칩니다. Cisco IOS CA 기능에 의해 생성된 인증서를 포함하는 CA(Certificate Authority)에서 생성한 인증서는 이 문제의 영향을 받지 않습니다.

영향을 받는 시스템

CSCvi48253이 없는 자체 서명 인증서를 사용하는 모든 IOS/IOS-XE 시스템 수정 또는 CSCvi48253이 없는 경우 SSC가 생성된 시간을 수정합니다. 여기에는 다음이 포함됩니다.

- 모든 IOS 12.x
- 15.6(3)M7, 15.7(3)M5, 15.8(3)M3, 15.9(3)M3 이전
- 모든 IOS-XE 16.9.1 이전

배경

Cisco IOS 및 Cisco IOS XE 소프트웨어의 특정 기능은 암호화 ID 검증을 위해 디지털 서명 X.509 인증서를 사용합니다. 이러한 인증서는 외부 서드파티 CA에 의해 생성되거나 Cisco IOS 또는 Cisco IOS XE 디바이스 자체에서 자체 서명 인증서로 생성될 수 있습니다. 영향을 받는 Cisco IOS 및 Cisco IOS XE 소프트웨어 릴리스는 항상 자체 서명 인증서의 만료 날짜를 2020-01-01 00:00:00 UTC로 설정합니다. 이 날짜 이후에는 인증서가 만료되고 유효하지 않습니다.

자체 서명 인증서를 사용할 수 있는 서비스는 다음과 같습니다.

일반 기능:

- HTTP Server over TLS(HTTPS) - HTTPS는 인증서가 만료되었음을 나타내는 오류를 브라우저에 생성합니다.
- SSH 서버 - X.509 인증서를 사용하여 SSH 세션을 인증하는 사용자가 인증에 실패할 수 있습니다. (X.509 인증서는 거의 사용하지 않습니다. 사용자 이름/비밀번호 인증 및 공개/개인 키 인증은 영향을 받지 않습니다.)
- RESTCONF - RESTCONF 연결이 실패할 수 있습니다.

협업 기능:

- TLS를 통한 SIP(Session Initiation Protocol)
- 암호화된 신호 처리가 활성화된 Cisco CME(Unified Communications Manager Express)
- 암호화된 신호 처리가 활성화된 Cisco SRST(Unified Survivable Remote Site Telephony)
- 암호화된 신호 처리가 활성화된 Cisco IOS dspfarm 리소스(컨퍼런스, 미디어 종료 지점 또는 트랜스코딩)
- 암호화된 시그널링으로 구성된 SCCP(Skinny Client Control Protocol) STCAPP(Telephony Control Application) 포트
- 사전 공유 키 없이 IP 보안(IPSec)을 통한 MGCP(Media Gateway Control Protocol) 및 H.323 통화 신호 처리
- 보안 모드의 Cisco Unified Communications Gateway Services API(HTTPS 사용)

무선 기능:

- 이전 Cisco IOS 액세스 포인트(2005 이전 버전에서 제조)와 Wireless LAN Controller 간의 LWAPP/CAPWAP 연결 자세한 내용은 Cisco Field Notice FN63942를 참조하십시오.

문제 증상

2020-01-01 00:00:00 UTC 이후 영향받는 Cisco IOS 또는 Cisco IOS XE 소프트웨어 릴리스에서 자

체 서명 인증서를 생성하려고 하면 다음 오류가 발생합니다.

```
../cert-c/source/certobj.c(535) : E_VALIDITY : validity period start later than end
```

자체 서명 인증서를 사용하는 모든 서비스는 작동하지 않을 수 있습니다. 예를 들면 다음과 같습니다.

- SIP over TLS 호출이 완료되지 않습니다.
- 암호화된 신호 처리가 활성화된 Cisco Unified CME에 등록된 디바이스는 더 이상 작동하지 않습니다.
- 암호화된 신호 처리가 활성화된 Cisco Unified SRST는 디바이스를 등록할 수 없습니다.
- 암호화된 신호 처리가 활성화된 Cisco IOS dspfarm 리소스(컨퍼런스, 미디어 종료 지점 또는 트랜스코딩)는 더 이상 등록되지 않습니다.
- 암호화된 시그널링을 사용하여 구성된 STCAPP 포트는 더 이상 등록되지 않습니다.
- 사전 공유 키 없이 IPSec을 통한 MGCP 또는 H.323 통화 시그널링을 사용하는 게이트웨이를 통한 통화는 실패합니다.
- 보안 모드(HTTPS 사용)에서 Cisco Unified Communications Gateway Services API를 사용하는 API 호출이 실패합니다.
- RESTCONF가 실패할 수 있습니다.
- 디바이스를 관리하는 HTTPS 세션에는 인증서가 만료되었음을 나타내는 브라우저 경고가 표시됩니다.
- AnyConnect SSL VPN 세션이 유효하지 않은 인증서를 설정하거나 보고하지 못합니다.
- IPSec 연결이 설정되지 않습니다.

영향을 받는 제품을 식별하는 방법

참고: 이 필드 알림의 영향을 받으려면 장치에 자체 서명 인증서가 정의되어 있어야 하며, 아래에 설명된 하나 이상의 기능에 자체 서명 인증서를 적용해야 합니다. 자체 서명 인증서만 있으면 인증서가 만료될 때 디바이스의 작동에 영향을 주지 않으며 즉각적인 조치가 필요하지 않습니다. **영향을 받으려면 디바이스가 아래의 3단계 및 4단계의 *모두* 기준을 충족해야 합니다.**

자체 서명 인증서를 사용하는지 확인하려면 다음 단계를 완료하십시오.

1. show running-**config 입력 |** 디바이스에서 crypto 명령을 시작합니다.

2. crypto PKI 신뢰 지점 컨피그레이션을 찾습니다.
3. crypto PKI trustpoint 컨피그레이션에서 trustpoint 등록 컨피그레이션을 확인합니다. 신뢰 지점 등록은 "**셀프 서명**"에 영향을 받도록 구성해야 합니다. 또한 자체 서명 인증서도 컨피그레이션에 나타나야 합니다. *신뢰 지점 이름에는 이 예와 같이 "self-signed"라는 단어가 포함되지 않을 수 있습니다.*

```
crypto pki trustpoint TP-self-signed-XXXXXXXX
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-662415686
  revocation-check none
  rsakeypair TP-self-signed-662415686
!
!
crypto pki certificate chain TP-self-signed-XXXXXXXX
certificate self-signed 01
  3082032E 31840216 A0030201 02024101 300D0609 2A864886 F70D0101 05050030
  30312E30 2C060355 04031325 494A531D 53656C66 2D536967 6E65642D 43657274
  ...
  ECA15D69 11970A66 252D34DC 760294A6 D1EA2329 F76EB905 6A5153C9 24F2958F
```

```
D19BFB22 9F89EE23 02D22D9D 2186B1A1 5AD4
```

신뢰 지점 등록이 "selfsigned"에 대해 구성되지 *않은* **경우 - 이 필드 알림의 영향을 받지 않습니다**. 별도의 조치가 필요하지 않습니다.**신뢰 지점 등록***이* **"selfsigned"에 대해 구성되어 있고 자체 서명 인증서가 컨피그레이션에 나타나는 경우 -** 디바이스가 이 필드 알림의 영향을 받을 **수 있습니다**. 4단계로 진행합니다.

4. 3단계에서 신뢰 지점 등록이 "selfsigned"에 대해 구성되어 있고 자체 서명 인증서가 컨피그레이션에 나타나는지 확인한 경우, 자체 서명 인증서가 디바이스의 기능에 적용되었는지 확인합니다.

   SSC에 연결될 수 있는 다양한 기능이 다음 샘플 컨피그레이션에 표시됩니다.

- **HTTPS 서버의 경우** 이 텍스트가 있어야 합니다.

```
ip http secure-server
```

또한 아래와 같이 신뢰 지점을 정의할 수도 있습니다. 아래 명령이 없으면 **기본 동작은 자체 서명 인증서를 사용하는 것입니다**.

```
ip http secure-trustpoint TP-self-signed-XXXXXXXX
```

신뢰 지점이 정의되고 자체 서명 인증서 이외의 인증서를 가리키는 경우 영향을 받지 않습니다.

HTTPS 서버의 경우 **만료된 인증서의 영향은** 웹 브라우저에서 자체 서명된 인증서를 이미 신뢰할 수 없으므로 **사소한** 것이며 만료되지 않은 경우에도 경고를 생성합니다. 만료된 인증서가 있으면 브라우저에서 수신하는 경고가 변경될 수 있습니다.

- **SIP over TLS**의 경우 이 텍스트는 구성 파일에 표시됩니다.

```
voice service voip
 sip
  session transport tcp tls
!
sip-ua
crypto signaling default trustpoint <self-signed-trustpoint-name>
! or
crypto signaling remote-addr a.b.c.d /nn trustpoint <self-signed-trustpoint-name>
!
```

- **암호화된 신호 처리가 활성화된 Cisco Unified CME**의 경우 이 텍스트는 구성 파일에 표시됩니다.

```
telephony-service
 secure-signaling trustpoint <self-signed-trustpoint-name>
 tftp-server-credentials trustpoint <self-signed-trustpoint-name>
```

- **암호화된 신호 처리가 활성화된 Cisco Unified SRST**의 경우 이 텍스트는 구성 파일에 표시됩니다.

```
credentials
 trustpoint <self-signed-trustpoint-name>
```

- **암호화된 신호 처리가 활성화된 Cisco IOS dspfarm 리소스(Conference, Media Termination Point 또는 Transcoding)**의 경우 이 텍스트는 컨피그레이션 파일에 표시됩니다.

```
dspfarm profile 1 conference security
trustpoint <self-signed-trustpoint-name>
!
```

```
dspfarm profile 2 mtp security
trustpoint <self-signed-trustpoint-name>
!
dspfarm profile 3 transcode security
 trustpoint <self-signed-trustpoint-name>
!
sccp ccm 127.0.0.1 identifier 1 priority 1 version 7.0 trustpoint <self-signed-trustpoint-
name>
!
```

- **암호화된 시그널링을 사용하여 구성된 STCAPP 포트**의 경우 이 텍스트는 컨피그레이션 파일에 표시됩니다.

```
stcapp security trustpoint <self-signed-trustpoint-name>
stcapp security mode encrypted
```

- **보안 모드의 Cisco Unified Communications Gateway Services API의 경우** 이 텍스트는 구성 파일에 표시됩니다.

```
uc secure-wsapi
ip http secure-server
ip http secure-trustpoint TP-self-signed-XXXXXXXX
```

- **SSLVPN**의 경우 이 텍스트는 구성 파일에 표시됩니다.

```
webvpn gateway <gw name>
 ssl trustpoint TP-self-signed-XXXXXXXX

OR

crypto ssl policy <policy-name>
pki trustpoint <trustpoint-name> sign
```

- **ISAKMP 및 IKEv2**의 **경우** 컨피그레이션이 있는 경우 자체 서명 인증서를 사용할 수 있습니다(해당 기능이 자체 서명 인증서를 사용하는지 다른 인증서와 사용하는지 확인하기 위해 컨피그레이션을 추가로 분석해야 함).

```
crypto isakmp policy <number>
 authentication pre-share | rsa-encr < NOT either of these
!
crypto ikev2 profile <prof name>
 authentication local rsa-sig
 pki trustpoint TP-self-signed-xxxxxx
!
crypto isakmp profile <prof name>
 ca trust-point TP-self-signed-xxxxxx
```

- **SSH 서버의 경우**, 참고: 인증서를 활용하여 SSH 세션을 인증하는 것은 거의 불가능합니다. 그러나 컨피그레이션을 확인하여 이를 확인할 수 있습니다. 영향을 받으려면 아래의 세 행이 모두 있어야 합니다. **참고 2: 사용자 이름과 비밀번호 조합을 사용하여 디바이스에 SSH를 사용하는 경우 영향을 받지 않습니다.**

```
ip ssh server certificate profile
 ! Certificate used by server
 server
  trustpoint sign TP-self-signed-xxxxxx
```

- **RESTCONF**의 경우 이 텍스트는 구성 파일에 표시됩니다.

```
restconf
! And one of the following ip http secure-trustpoint TP-self-signed-XXXXXXXXX ! OR ip http
client secure-trustpoint TP-self-signed-XXXXXXXX
```

해결 방법/솔루션

이 솔루션은 Cisco IOS 또는 Cisco IOS XE 소프트웨어를 다음 수정 사항이 포함된 릴리스로 업그레이드하는 것입니다.

- Cisco IOS XE Software 릴리스 16.9.1 이상
- Cisco IOS Software 릴리스 15.6(3)M7 이상 15.7(3)M5 이상 또는 15.8(3)M3 이상

소프트웨어를 업그레이드한 후 자체 서명 인증서를 다시 생성하고 해당 신뢰 저장소의 인증서가 필요할 수 있는 모든 디바이스로 내보내야 합니다.

즉시 소프트웨어 업그레이드를 수행할 수 없는 경우 3가지 해결 방법을 사용할 수 있습니다.

해결 방법 1 - 타사 CA(Certificate Authority)에서 유효한 인증서를 가져옵니다.

인증 기관에서 인증서를 설치합니다. 공통 CA에는 다음이 포함됩니다. Comodo, Let's Encrypt, RapidSSL, Thawte, Sectigo, GeoTrust, Symantec 및 기타 여러 가지

이 해결 방법을 사용하면 Cisco IOS에서 인증서 요청을 생성하고 표시합니다. 그런 다음 관리자는 요청을 복사하여 서드파티 CA에 제출하고 결과를 검색합니다.

참고: 인증서를 서명하는 데 CA를 사용하는 것은 보안 모범 사례로 간주됩니다. 이 절차는 이 필드 알림에 해결 방법으로 제공됩니다. 그러나 이 해결 방법을 적용한 후에 자체 서명 인증서를 사용하지 않고 서드파티 CA 서명 인증서를 계속 사용하는 것이 좋습니다.

타사 CA에서 인증서를 설치하려면 다음 단계를 완료하십시오.

1. CSR(Certificate Signing Request)을 생성합니다.

```
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# crypto pki trustpoint TEST
Router(ca-trustpoint)# enrollment term pem
Router(ca-trustpoint)# subject-name CN=TEST
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# rsakeypair TEST
Router(ca-trustpoint)# exit
Router(config)# crypto pki enroll TEST
% Start certificate enrollment ..
% The subject name in the certificate will include: CN=TEST
% The subject name in the certificate will include: Router.cisco.com
% The serial number in the certificate will be: FTX1234ABCD
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
-----BEGIN CERTIFICATE REQUEST-----
A Base64 Certificate is displayed here. Copy it, along with the ---BEGIN and ---END lines.
-----END CERTIFICATE REQUEST-----
---End - This line not part of the certificate request---
```

2. CSR을 서드파티 CA에 제출합니다.**참고:** CSR을 서드파티 CA에 제출하고 결과 인증서를 검색하는 절차는 사용 중인 CA에 따라 다릅니다. 이 단계를 수행하는 방법에 대한 지침은 CA 설명서를 참조하십시오.
3. CA 인증서와 함께 라우터의 새 ID 인증서를 다운로드합니다.
4. 디바이스에 CA 인증서를 설치합니다.

```
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# crypto pki auth TEST

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
REMOVED
-----END CERTIFICATE-----
```

```
Certificate has the following attributes:
   Fingerprint MD5: 79D15A9F C7EB4882 83AC50AC 7B0FC625
   Fingerprint SHA1: 0A80CC2C 9C779D20 9071E790 B82421DE B47E9006

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

5. 디바이스에 ID 인증서를 설치합니다.

```
Router(config)# crypto pki import TEST certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
REMOVED
-----END CERTIFICATE-----

% Router Certificate successfully imported
```

해결 방법 2 - IOS CA 서버를 사용하여 새 인증서를 생성합니다.

로컬 Cisco IOS Certificate Authority 서버를 사용하여 새 인증서를 생성하고 서명합니다.

참고: 로컬 CA 서버 기능은 일부 제품에서 사용할 수 없습니다.

```
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip http server
Router(config)# crypto pki server IOS-CA
Router(cs-server)# grant auto
Router(cs-server)# database level complete
Router(cs-server)# no shut
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password:
```

```
Router# show crypto pki server IOS-CA Certificates
Serial Issued date Expire date Subject Name
1 21:31:40 EST Jan 1 2020 21:31:40 EST Dec 31 2022 cn=IOS-CA
```

```
Router# conf t

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# crypto pki trustpoint TEST
Router(ca-trustpoint)# enrollment url http:// # Replace
```

```
Router(ca-trustpoint)# subject-name CN=TEST
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# rsakeypair TEST
Router(ca-trustpoint)# exit
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# crypto pki auth TEST
Certificate has the following attributes:
Fingerprint MD5: C281D9A0 337659CB D1B03AA6 11BD6E40
Fingerprint SHA1: 1779C425 3DCEE86D 2B11C880 D92361D6 8E2B71FF
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
Router(config)# crypto pki enroll TEST
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:
```

해결 방법 3 - OpenSSL을 사용하여 새 자체 서명 인증서를 생성합니다.

OpenSSL을 사용하여 PKCS12 인증서 번들을 생성하고 번들을 Cisco IOS로 가져옵니다.

LINUX, UNIX 또는 MAC(OSX) 예

```
User@linux-box$ openssl req -newkey rsa:2048 -nodes -keyout tmp.key -x509 -days 4000 -out
tmp.cer -subj
"/CN=SelfSignedCert" &> /dev/null && openssl pkcs12 -export -in tmp.cer -inkey tmp.key -out
tmp.bin
-passout pass:Cisco123 && openssl pkcs12 -export -out certificate.pfx -password pass:Cisco123 -
inkey
tmp.key -in tmp.cer && rm tmp.bin tmp.key tmp.cer && openssl base64 -in certificate.pfx
MIII8QIBAzCCCLcGCSqGSIb3DQEHAaCCCKgEggikMIIIoDCCA1cGCSqGSIb3DQEH
BqCCA0gwggNEAgEAMIIDPQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQIGnxm
t5r28FECAggAgIIDEKyw10smucdQGt1c0DdfYXwUo8BwaBnzQvN0ClawXNQln2bT
vrhus6LfRvVxBNPeQz2ADgLikGxatwV5EDgooM+IEucKDURGLEotaRrVU5Wk3EGM
mjC6Ko9OaM30vhAGEEXrk26cq+OWsEuF3qudggRYv2gIBcrJ2iUQNFsBIrvlGHRo
FphOTqhVaAPxZS7hOB30cK1tMKHOIa8EwygyBvQPfjjBT79QFgeexIJFmUtqYX/P
```

Cisco IOS 또는 IOS XE Router 예

```
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# crypto pki trustpoint TEST
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# exit
R1(config)#crypto pki import TEST pkcs12 terminal password Cisco123
Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
MIII8QIBAzCCCLcGCSqGSIb3DQEHAaCCCKgEggikMIIIoDCCA1cGCSqGSIb3DQEH
BqCCA0gwggNEAgEAMIIDPQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQItyCo
Vh05+0QCAggAgIIDENUWY+UeuY5sIRZuoBi2nEhdIPd1th/auBYtX79aXGiz/iEW
```

새 인증서가 설치되었는지 확인합니다.

```
R1#show crypto pki certificates TEST
Load for five secs: 5%/1%; one minute: 2%; five minutes: 3%
Time source is SNTP, 15:04:37.593 UTC Mon Dec 16 2019
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 00A16966E46A435A99
  Certificate Usage: General Purpose
  Issuer:
    cn=SelfSignedCert
  Subject:
    cn=SelfSignedCert
  Validity Date:
    start date: 14:54:46 UTC Dec 16 2019
    end   date: 14:54:46 UTC Nov 28 2030
```

추가 정보

FN70489 필드 알림 참조: FN - 70489 - Cisco IOS 및 Cisco IOS XE Software에서 PKI 자체 서명 인증서 만료

CSCvi48253 참조 자체 서명 인증서는 2020년 1월 1일 UTC에 만료되며, 그 이후에는 만들 수 없습니다.

질문과 대답

Q: 무엇이 문제입니까?

영향을 받는 Cisco IOS 또는 Cisco IOS-XE 버전을 실행하는 제품에서 생성된 자체 서명 X.509 PKI 인증서는 01/01/2020 00:00:00 UTC에 만료됩니다. 01/01/2020 00:00:00 UTC 이후에는 영향을 받는 디바이스에 새 자체 서명 인증서를 생성할 수 없습니다. 이러한 자체 서명 인증서에 의존하는 모든 서비스는 인증서가 만료된 후에 더 이상 작동하지 않을 수 있습니다.

Q: 제품의 자체 서명 인증서가 만료될 경우 고객 네트워크에 미치는 영향은 무엇입니까?

자체 서명 인증서를 사용하는 영향을 받는 제품의 기능은 인증서가 만료된 후에 더 이상 작동하지 않을 수 있습니다. 자세한 내용은 필드 알림을 참조하십시오.

Q: 이 문제의 영향을 받는지 어떻게 알 수 있습니까?

Field Notice(필드 알림)에서는 자체 서명 인증서를 사용하고 있는지 여부 및 컨피그레이션이 이 문제의 영향을 받는지 여부를 확인하는 지침을 제공합니다. Field Notice(필드 알림)의 "How To Identify Affected Products(영향받는 제품을 식별하는 방법)" 섹션을 참조하십시오.

Q: 제가 영향을 받았는지 확인하기 위해 실행할 수 있는 스크립트가 있나요?

예. Cisco CLI Analyzer를 사용하여 시스템 진단 실행을 실행합니다. 인증서가 있고 사용 중인 경우 경고가 표시됩니다. https://cway.cisco.com/cli/

Q. Cisco에서 이 문제에 대한 소프트웨어 수정 사항을 제공했습니까?

예. Cisco는 소프트웨어 업그레이드가 즉시 가능하지 않을 경우 이 문제에 대한 소프트웨어 수정 사항과 해결 방법을 발표했습니다. 자세한 내용은 필드 알림을 참조하십시오.

Q: 이 문제는 인증서를 사용하는 Cisco 제품에 영향을 미칩니까?

아니요. 이 문제는 **특정 버전의 Cisco IOS 또는 Cisco IOS-XE에서 생성한 자체 서명 인증서를 사용하는 제품에만** 영향을 **미치며**, 이 인증서는 제품의 서비스에 적용됩니다. CA(Certificate Authority)에서 생성한 인증서를 사용하는 제품은 이 문제의 영향을 받지 않습니다.

Q: Cisco 제품은 자체 서명 인증서만 사용합니까?

아니요. 인증서는 외부 서드파티 인증 기관에서 생성할 수도 있고, Cisco IOS 또는 Cisco IOS-XE 장치 자체에서 자체 서명 인증서로 생성할 수도 있습니다. 특정 고객 요구 사항으로 인해 자체 서명 인증서를 사용할 수 있습니다. CA(Certificate Authority)에서 생성한 인증서는 이 문제의 영향을 받지 않습니다.

Q. 이 문제는 왜 발생했습니까?

안타깝게도, 기술 공급업체의 최선의 노력에도 불구하고 소프트웨어 결함은 여전히 발생합니다. 어떤 Cisco 기술에서도 버그가 발견되면, Cisco는 투명성을 유지하고 고객에게 네트워크를 보호하는 데 필요한 정보를 제공하기 위해 노력하고 있습니다.

이 경우, Cisco IOS 및 Cisco IOS-XE의 영향을 받는 버전이 항상 자체 서명 인증서의 만료 날짜를 01/01/2020 00:00:00 UTC로 설정하는 알려진 소프트웨어 버그로 인해 문제가 발생합니다. 이 날짜 이후에는 인증서가 만료되고 유효하지 않으므로 제품 기능에 영향을 미칠 수 있습니다.

Q: 2020년 1월 1일 00:00:00 UTC의 만료일이 선택된 이유는 무엇입니까?

일반적으로 인증서는 만료 날짜를 갖습니다. 이 소프트웨어 버그의 경우, 2020년 1월 1일은 10년 전에 Cisco IOS 및 Cisco IOS-XE 소프트웨어 개발 중에 사용되었으며 사람의 실수입니다.

Q: 이 문제의 영향을 받는 제품은 무엇입니까?

15.6(03)M07, 15.7(03)M05, 15.8(03)M03, 15.9(03)M 및 16.9.1 이전 버전의 Cisco IOS-XE 릴리스를 실행하는 모든 Cisco 제품

Q: 고객은 무엇을 해야 합니까?

Cisco는 고객에게 현장 공지를 검토하여 이 문제의 영향을 받는지 여부를 평가하고, 그렇다면 해결 방법/솔루션 지침을 따라 이 문제를 완화하도록 요청합니다.

Q: 이 문제가 보안 취약성입니까?

아니요. 이는 보안 취약성이 아니며 제품의 무결성에 대한 위험이 없습니다.

Q: SSH가 영향을 받습니까?

아니요. SSH는 RSA 키 쌍을 사용하지만 드문 컨피그레이션을 제외하고 인증서를 사용하지 않습니다. IOS에서 인증서를 사용하려면 다음 컨피그레이션이 있어야 합니다.

```
ip ssh server certificate profile
   server
      trustpoint sign TP-self-signed-xxxxxx
```

Q: 기존 Catalyst 2K, 3K, 4K, 6K 플랫폼에 사용할 수 있는 고정 버전은 무엇입니까?

Polaris 기반 플랫폼(3650/3850/Catalyst 9K 시리즈)의 경우 16.9.1 이후 수정 가능
CDB 플랫폼의 경우 15.2(7)E1a를 계속 사용할 수 있습니다.

다른 기존 스위칭 플랫폼의 경우:

커밋이 진행 중이지만 CCO 릴리스를 게시하지 않았습니다. 다음 CCO 릴리스에 수정 사항이 있습니다.

이 시간대에는 다른 해결 방법 중 하나를 활용하십시오.

Q: WAAS가 영향을 받습니까?

WAAS는 계속해서 정상적으로 작동하고 트래픽을 최적화하지만, AppNav-XE 및 Central Manager는 만료된 자체 서명 인증서가 있는 장치로 오프라인 상태가 됩니다. 즉, AppNav-Cluster를 모니터링하거나 WAAS에 대한 정책을 변경할 수 없습니다. 요약하면, WAAS는 계속해서 정상적으로 작동하지만 인증서 문제가 해결될 때까지 관리 및 모니터링이 일시 중단됩니다. 문제를 해결하려면 IOS에서 새 인증서를 생성한 다음 중앙 관리자로 가져와야 합니다.