IOS - Selbstsigniertes Zertifikat läuft am 1. Januar 2020 ab

Inhalt

Einleitung

In diesem Dokument werden die Auswirkungen und Fehler beschrieben, die durch das Ablaufdatum der selbstsignierten Zertifikate (SSC) auf Cisco Softwaresystemen verursacht werden. Darüber hinaus werden verschiedene Problemumgehungen beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Selbstsignierte Zertifikate (SSC)
- Cisco IOS® Version 12.x und höher

Verwendete Komponenten

Die Komponenten sind die Softwaresysteme, die vom Ablauf des SSC betroffen sind.

Alle Cisco IOS- und Cisco IOS® XE-Systeme, die ein selbstsigniertes Zertifikat verwenden, die nicht über die Cisco Bug-ID CSCvi48253 verfügen oder die beim Generieren der SSC nicht die Cisco Bug-ID CSCvi48253 aufweisen. Dazu gehören:

- Alle Cisco IOS 12.x
- Alle Cisco IOS 15.x-Versionen vor 15.6(3)M7, 15.7(3)M5, 15.8(3)M3, 15.9(3)M
- Alle Cisco IOS XE Versionen vor 16.9.1

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrund

> **Anmerkung:** Dieses Dokument enthält den Inhalt von FN40789 sowie zusätzlichen Kontext, Beispiele, Updates und Fragen und Antworten.

Am 1. Januar 2020 um 00:00 Uhr UTC liefen alle auf Cisco IOS- und Cisco IOS XE-Systemen generierten selbstsignierten Zertifikate ab, es sei denn, auf dem System wurde beim Generieren des SSC eine feste Version von Cisco IOS und Cisco IOS XE ausgeführt. Danach können nicht korrigierte Cisco IOS-Systeme keine neuen SSCs mehr generieren. Jeder Dienst, der diese selbstsignierten Zertifikate benötigt, um eine sichere Verbindung herzustellen oder zu beenden, funktioniert nach Ablauf des Zertifikats nicht mehr.

Dieses Problem betrifft nur selbstsignierte Zertifikate, die vom Cisco IOS- oder Cisco IOS XE-Gerät generiert und auf einen Dienst auf dem Gerät angewendet wurden. Zertifikate, die von einer Zertifizierungsstelle (Certificate Authority, CA) generiert wurden, die die Zertifikate enthält, die von der Funktion der Cisco IOS-Zertifizierungsstelle generiert wurden, sind von diesem Problem nicht betroffen.

Einige Funktionen der Cisco IOS- und Cisco IOS XE-Software basieren auf digital signierten X.509-Zertifikaten für die kryptografische Identitätsvalidierung. Diese Zertifikate werden entweder von einer externen Zertifizierungsstelle eines Drittanbieters oder auf dem Cisco IOS- oder Cisco IOS XE-Gerät selbst als selbstsigniertes Zertifikat generiert. Betroffene Softwareversionen von Cisco IOS und Cisco IOS XE setzen das Ablaufdatum des selbstsignierten Zertifikats auf

1.01.2020, 00:00:00 UTC. Nach diesem Datum läuft das Zertifikat ab und ist ungültig.

Folgende Dienste können sich auf ein selbstsigniertes Zertifikat verlassen:

Allgemeine Funktionen

- HTTP Server over TLS (HTTPS) - HTTPS löst einen Browser-Fehler aus, der darauf hinweist, dass das Zertifikat abgelaufen ist.
- SSH-Server - Benutzer, die X.509-Zertifikate zur Authentifizierung der SSH-Sitzung verwenden, können die Authentifizierung versagen. (Die Verwendung von X.509-Zertifikaten ist selten. Benutzername/Passwort-Authentifizierung und Authentifizierung mit öffentlichem/privatem Schlüssel sind nicht betroffen.)
- RESTCONF - RESTCONF-Verbindungen können fehlschlagen.

Collaboration-Funktionen

- Session Initiation Protocol (SIP) über TLS
- Cisco Unified Communications Manager Express (CME) mit aktivierter verschlüsselter Signalisierung
- Cisco Unified Survivable Remote Site Telefony (SRST) mit aktivierter verschlüsselter Signalisierung
- Cisco IOS dspfarm Ressourcen (Konferenz, Media Termination Point oder Transcoding) mit aktivierter verschlüsselter Signalisierung
- SCCP-Ports (Skinny Client Control Protocol) der Telefony Control Application (STCAPP), die mit verschlüsselter Signalisierung konfiguriert sind
- Media Gateway Control Protocol (MGCP) und H.323 Call Signaling over IP Security (IPSec) ohne Pre-Shared Key
- Cisco Unified Communications Gateway Services API im abgesicherten Modus (mit HTTPS)

Wireless-Funktionen

- LWAPP/CAPWAP-Verbindungen zwischen älteren Cisco IOS Access Points (2005 oder älter hergestellt) und Wireless LAN Controller. Weitere Informationen finden Sie in der Cisco Problemhinweis-E-Mail FN63942.

Problem

Der Versuch, ein selbstsigniertes Zertifikat für eine betroffene Cisco IOS- oder Cisco IOS XE-Softwareversion nach dem 1.1.2020 um 00:00:00 UTC zu generieren, führt zu folgendem Fehler:

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

Dienste, die auf dem selbstsignierten Zertifikat basieren, funktionieren nicht. Beispiele:

- SIP über TLS-Anrufe werden nicht abgeschlossen.
- Bei Cisco Unified CME registrierte Geräte mit aktivierter verschlüsselter Signalisierung funktionieren nicht mehr.

- Cisco Unified SRST mit aktivierter verschlüsselter Signalisierung ermöglicht den Geräten die Registrierung nicht.
- Die Cisco IOS dspfarm-Ressourcen (Conference, Media Termination Point oder Transcoding) mit aktivierter verschlüsselter Signalisierung registrieren sich nicht mehr.
- Mit verschlüsselter Signalisierung konfigurierte STCAPP-Ports registrieren sich nicht mehr.
- Anrufe über ein Gateway, die MGCP- oder H.323-Anrufsignalisierung über IPSec ohne Pre-Shared Key umfassen, können fehlschlagen.
- API-Aufrufe, die die Cisco Unified Communications Gateway Services-API im gesicherten Modus (mit HTTPS) verwenden, können fehlschlagen.
- RESTCONF kann fehlschlagen.
- HTTPS-Sitzungen zur Verwaltung des Geräts zeigen eine Browserwarnung an, die darauf hinweist, dass das Zertifikat abgelaufen ist.
- Bei AnyConnect SSL VPN-Sitzungen kann kein ungültiges Zertifikat erstellt oder gemeldet werden.
- IPSec-Verbindungen können sich nicht herstellen.

Identifizierung betroffener Produkte

> **Anmerkung:** Um von dieser Meldung betroffen zu sein, muss für ein Gerät ein selbstsigniertes Zertifikat definiert sein, *und* das selbstsignierte Zertifikat muss auf eine oder mehrere der folgenden Funktionen angewendet werden. Das Vorhandensein eines selbstsignierten Zertifikats allein hat keine Auswirkungen auf den Betrieb des Geräts nach Ablauf des Zertifikats und erfordert keine sofortigen Maßnahmen. **Um betroffen zu sein, muss ein Gerät die Kriterien in Schritt 3 und Schritt 4 unten erfüllen.**

So prüfen Sie, ob Sie ein selbstsigniertes Zertifikat verwenden:

1. Geben Sie show running-config | begin crypto auf Ihrem Gerät.
2. Suchen Sie nach der Konfiguration des Crypto PKI-Vertrauenspunkts.
3. Suchen Sie in der Konfiguration des Crypto PKI-Vertrauenspunkts nach der Konfiguration für die Registrierung des Vertrauenspunkts. Die TrustPoint-Registrierung muss konfiguriert werden, damit sich "**selbst signiert**" auswirken kann. Außerdem muss das selbstsignierte Zertifikat in der Konfiguration angezeigt werden. Beachten Sie, dass der Name des Vertrauenspunkts nicht die Worte "selbst signiert" enthält, wie im folgenden Beispiel gezeigt.

```
crypto pki trust-point 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
```

> **Wenn die Registrierung des Vertrauenspunkts** *nicht* **für "**selbstsigniert" **konfiguriert ist, hat dieser Problemhinweis KEINE Auswirkungen auf das Gerät**. Es sind keine Maßnahmen erforderlich.**Wenn die Registrierung des Vertrauenspunkts für "selbstsigniert" konfiguriert** *ist* **und das selbstsignierte Zertifikat in der Konfiguration angezeigt wird, kann** das **Gerät** durch diesen Problemhinweis **beeinträchtigt werden**. Fahren Sie mit Schritt 4 fort.

4. Wenn Sie in Schritt 3 festgestellt haben, dass die Vertrauenspunktregistrierung für "selbstsigniert" konfiguriert ist und dass das selbstsignierte Zertifikat in der Konfiguration angezeigt wird, prüfen Sie, ob das selbstsignierte Zertifikat auf eine Funktion auf dem Gerät angewendet wird.In den folgenden Beispielkonfigurationen werden verschiedene Funktionen veranschaulicht, die an den SSC gebunden werden können:

- Für **HTTPS-Server** muss dieser Text vorhanden sein:

```
ip http secure-server
```

Zusätzlich kann ein Vertrauenspunkt definiert werden, wie im nächsten Codebeispiel gezeigt. Wenn dieser Befehl nicht vorhanden ist, wird standardmäßig das selbstsignierte Zertifikat verwendet.

```
ip http secure-trust-point TP-self-signed-XXXXXXXX
```

Wenn ein Vertrauenspunkt definiert ist und auf ein anderes Zertifikat als das selbstsignierte Zertifikat verweist, sind Sie davon nicht betroffen.

Bei **HTTPS-Servern** sind die Auswirkungen des abgelaufenen Zertifikats gering, da selbstsignierte Zertifikate von Webbrowsern bereits nicht mehr vertrauenswürdig sind und eine Warnung auslösen, auch wenn sie nicht abgelaufen sind. Das Vorhandensein eines abgelaufenen Zertifikats kann die Warnung ändern, die Sie im Browser erhalten.

- Bei **SIP über TLS** ist dieser Text in der Konfigurationsdatei enthalten:

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

- Bei **Cisco Unified CME** mit aktivierter verschlüsselter Signalisierung wird dieser Text in der Konfigurationsdatei angezeigt:

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

- Bei **Cisco Unified SRST** mit aktivierter verschlüsselter Signalisierung ist dieser Text in der Konfigurationsdatei enthalten:

```
credentials
 trust-point <self-signed-trust-point-name>
```

- für **Cisco IOS dspfarm Ressource**s (Konferenz, Media Termination Point oder Transcoding) bei aktivierter verschlüsselter Signalisierung wird dieser Text in der Konfigurationsdatei angezeigt:

```
dspfarm profile 1 conference security
trust-point <self-signed-trust-point-name>
!
dspfarm profile 2 mtp security
trust-point <self-signed-trust-point-name>
```

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

- Bei **STCAPP-Ports**, die mit verschlüsselter Signalisierung konfiguriert sind, ist dieser Text in der Konfigurationsdatei enthalten:
```
stcapp security trust-point <self-signed-trust-point-name>
stcapp security mode encrypted
```
- Für die **Cisco Unified Communications Gateway Services-API im abgesicherten Modus** ist dieser Text in der Konfigurationsdatei vorhanden:
```
uc secure-wsapi
ip http secure-server
ip http secure-trust-point TP-self-signed-XXXXXXXX
```
- Für **SSL VPN** ist dieser Text in der Konfigurationsdatei vorhanden:
```
webvpn gateway <gw name>
 ssl trust-point TP-self-signed-XXXXXXXX

OR

crypto ssl policy <policy-name>
pki trust-point <trust-point-name> sign
```
- Für **ISAKMP und IKEv2** kann das selbstsignierte Zertifikat verwendet werden, wenn eine der Konfigurationen vorhanden ist (weitere Analysen der Konfiguration sind erforderlich, um zu ermitteln, ob für die Funktion das selbstsignierte Zertifikat anstatt eines anderen Zertifikats verwendet wird):
```
crypto isakmp policy <number>
 authentication pre-share | rsa-encr < NOT either of these
!
crypto ikev2 profile <prof name>
 authentication local rsa-sig
 pki trust-point TP-self-signed-xxxxxx
!
crypto isakmp profile <prof name>
 ca trust-point TP-self-signed-xxxxxx
```
- Für **SSH-Server** ist es äußerst unwahrscheinlich, dass Sie Zertifikate zur Authentifizierung der SSH-Sitzungen verwenden können. Sie können diese Konfiguration jedoch überprüfen. Im nächsten Codebeispiel müssen alle drei Zeilen angezeigt werden, damit sie betroffen sind. **Anmerkung:** Wenn Sie die Kombination aus Benutzername und Kennwort für SSH auf Ihrem Gerät verwendet haben, sind Sie NICHT betroffen.
```
ip ssh server certificate profile
 ! Certificate used by server
 server
  trust-point sign TP-self-signed-xxxxxx
```
- Für **RESTCONF** ist dieser Text in der Konfigurationsdatei vorhanden:
```
restconf
! And one of the following ip http secure-trust-point TP-self-signed-XXXXXXXXX ! OR ip http
client secure-trust-point TP-self-signed-XXXXXXXX
```

Lösung(en)

Die Lösung besteht darin, die Cisco IOS- oder Cisco IOS XE-Software auf eine Version zu aktualisieren, die den folgenden Fix enthält:

- Cisco IOS XE Softwareversion 16.9.1 und höher
- Cisco IOS Software, Version 15.6(3)M7 und höher 15.7(3)M5 und spätere Version oder 15.8(3)M3 und höher

Nachdem Sie die Software aktualisiert haben, müssen Sie das selbstsignierte Zertifikat neu generieren und auf alle Geräte exportieren, die das Zertifikat in ihrem Vertrauensspeicher benötigen.

Wenn ein sofortiges Software-Upgrade nicht möglich ist, stehen drei Problemumgehungen zur Verfügung:

1. Beschaffen Sie sich ein gültiges Zertifikat von einer Zertifizierungsstelle des Drittanbieters.
2. Erstellen Sie mit dem Cisco IOS CA Server ein neues Zertifikat.
3. Verwenden Sie OpenSSL, um ein neues selbstsigniertes Zertifikat zu erstellen.

1. Erhalten Sie ein gültiges Zertifikat von einer Zertifizierungsstelle eines Drittanbieters

Installieren eines Zertifikats von einer Zertifizierungsstelle Zu den gängigen Zertifizierungsstellen gehören: Comodo, Let's Encrypt, RapidSSL, Thawte, Sectigo, GeoTrust, Symantec usw. Bei dieser Problemumgehung wird eine Zertifikatanforderung generiert und von Cisco IOS angezeigt. Anschließend kopiert der Administrator die Anforderung, sendet sie an eine Drittanbieter-Zertifizierungsstelle und ruft das Ergebnis ab.

> **Anmerkung:** Die Verwendung einer Zertifizierungsstelle zum Signieren von Zertifikaten gilt als Best Practice im Bereich Sicherheit. Dieses Verfahren dient als Workaround in dieser Problembeschreibung. Es ist jedoch vorzuziehen, das von der Zertifizierungsstelle signierte Zertifikat eines Drittanbieters auch nach Anwendung dieser Problemumgehung zu verwenden, anstatt ein selbstsigniertes Zertifikat zu verwenden.

So installieren Sie ein Zertifikat von einer Drittanbieter-Zertifizierungsstelle:

1. Erstellen einer Zertifikatsanforderung (Certificate Signing Request, CSR):

```
Router#configure terminal
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]: n
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---
```

1. Übermitteln Sie den CSR an die Drittanbieter-Zertifizierungsstelle.**Anmerkung:** Das Verfahren

zum Übermitteln des CSR an eine Drittanbieterzertifizierungsstelle und Abrufen des resultierenden Zertifikats hängt von der verwendeten Zertifizierungsstelle ab. Anweisungen zur Durchführung dieses Schrittes finden Sie in der Dokumentation für Ihre Zertifizierungsstelle.

2. Laden Sie das neue Identitätszertifikat für den Router zusammen mit dem Zertifizierungsstellenzertifikat herunter.
3. Installieren Sie das Zertifizierungsstellenzertifikat auf dem Gerät:

```
Router#configure terminal
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
trust-point CA certificate accepted.
% Certificate successfully imported
```

4. Installieren Sie das Identitätszertifikat auf dem Gerät:

```
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
```

2. Erstellen Sie mit dem Cisco IOS CA Server ein neues Zertifikat.

Verwenden Sie den lokalen Cisco IOS Certificate Authority-Server, um ein neues Zertifikat zu erstellen und zu signieren.

Hinweis: Die Funktion für den lokalen CA-Server ist nicht für alle Produkte verfügbar.

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

```
             <<<< Replace
```

```
subject-name CN=TEST
```

```
Router(ca-trustpoint)# revocation-check none
```

```
Router(ca-trustpoint)# rsakeypair TEST
```

```
Router(ca-trustpoint)# exit
```

```
Router# configure terminal
```

```
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 take note of it.
Password:
```

yes

```
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose TEST' command will show the fingerprint
```

3. OpenSSL verwenden, um ein neues selbstsigniertes Zertifikat zu generieren

Verwenden Sie OpenSSL, um ein PKCS12-Zertifikatpaket zu generieren und in Cisco IOS zu importieren.

Beispiel für LINUX, UNIX oder MAC (OSX)

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
```

Beispiel für einen Cisco IOS- oder Cisco IOS XE-Router

Router#**configure terminal**

```
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
```

Überprüfen Sie, ob das neue Zertifikat installiert ist:

```
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
```

> **Anmerkung:** Selbstsignierte Zertifikate laufen am 00:00 1 Jan 2020 UTC ab und können danach nicht mehr erstellt werden.

Fragen und Antworten

F: Worum geht es?

Selbstsignierte X.509 PKI-Zertifikate, die für Produkte generiert werden, auf denen betroffene Cisco IOS- oder Cisco IOS XE-Versionen ausgeführt werden, laufen am 01.01.2020 00:00:00 UTC ab. Nach dem 01.01.2020 um 00:00:00 UTC können auf den betroffenen Geräten keine neuen selbstsignierten Zertifikate mehr erstellt werden. Jeder Dienst, der auf diesen selbstsignierten Zertifikaten basiert, kann nach Ablauf des Zertifikats nicht mehr funktionieren.

F: Welche Auswirkungen hat es auf ein Client-Netzwerk, wenn ein selbstsigniertes Zertifikat für sein Produkt abläuft?

Die Funktionalität eines betroffenen Produkts, die auf den selbstsignierten Zertifikaten beruht, kann nach Ablauf des Zertifikats nicht mehr funktionieren. Weitere Informationen finden Sie in der Problembeschreibung.

F: Woher weiß ich, ob ich von diesem Problem betroffen bin?

In der Problemhinweis-Meldung wird erläutert, ob Sie ein selbstsigniertes Zertifikat verwenden und ob sich dieses Problem auf Ihre Konfiguration auswirkt. Weitere Informationen finden Sie in der Problembeschreibung im Abschnitt "Identifizieren betroffener Produkte".

F: Gibt es ein Skript, das ich ausführen kann, um festzustellen, ob ich betroffen bin?

Ja. Verwenden Sie Cisco CLI Analyzer, und führen Sie einen Systemdiagnosevorgang aus. Wenn das Zertifikat vorhanden ist und verwendet wird, kann eine Warnung angezeigt werden. https://cway.cisco.com/cli/

Frage: Hat Cisco Software-Patches für dieses Problem bereitgestellt?

Ja. Cisco hat zur Behebung dieses Problems Behebung von Softwareproblemen bereitgestellt und Workarounds bereitgestellt, falls ein Software-Upgrade nicht sofort durchführbar ist. Weitere Informationen finden Sie in der Problembeschreibung.

F: Betrifft dieses Problem Cisco Produkte, die ein Zertifikat verwenden?

Nein. Dieses Problem betrifft **nur Produkte, die selbstsignierte Zertifikate verwenden, die von bestimmten Versionen von Cisco IOS oder Cisco IOS XE generiert wurden,** wobei das Zertifikat auf einen Service auf dem Produkt angewendet wird. Produkte, die von einer Zertifizierungsstelle (Certificate Authority, CA) generierte Zertifikate verwenden, sind von diesem Problem nicht betroffen.

F: Verwenden Cisco Produkte nur selbstsignierte Zertifikate?

Nein. Zertifikate können entweder von einer externen Zertifizierungsstelle eines Drittanbieters oder auf dem Cisco IOS- oder Cisco IOS XE-Gerät selbst als selbstsigniertes Zertifikat generiert werden. Für bestimmte Benutzeranforderungen können selbstsignierte Zertifikate erforderlich sein. Zertifikate, die von einer Zertifizierungsstelle (Certificate Authority, CA) generiert wurden, sind von diesem Problem nicht betroffen.

Frage: Warum ist dieses Problem aufgetreten?

Leider treten trotz aller Bemühungen der Technologieanbieter immer noch Softwarefehler auf. Wenn ein Fehler in einer Cisco Technologie entdeckt wird, verpflichten wir uns zur Transparenz und stellen unseren Benutzern die Informationen bereit, die sie zum Schutz ihres Netzwerks benötigen.

In diesem Fall wird das Problem durch einen bekannten Softwarefehler verursacht, bei dem betroffene Versionen von Cisco IOS und Cisco IOS XE das Ablaufdatum des selbstsignierten Zertifikats immer auf 01.01.2020 00:00:00 UTC setzen können. Nach diesem Datum läuft das Zertifikat ab und ist ungültig. Dies kann sich auf die Produktfunktionalität auswirken.

F: Warum wurde das Ablaufdatum 1. Januar 2020 00:00:00 UTC gewählt?

Zertifikate haben in der Regel ein Ablaufdatum. Im Fall dieses Softwarefehlers wurde das Datum 1. Januar 2020 während der Softwareentwicklung von Cisco IOS und Cisco IOS XE vor über 10 Jahren verwendet. Es handelt sich hierbei um einen menschlichen Fehler.

F: Welche Produkte sind von diesem Problem betroffen?

Alle Cisco Produkte mit Cisco IOS-Versionen vor 15.6(03)M07, 15.7(03)M05, 15.8(03)M03 und 15.9(03)M sowie alle Cisco Produkte mit Cisco IOS XE-Versionen vor 16.9.1

F: Was müssen Benutzer tun?

Sie müssen den Problemhinweis lesen, um zu beurteilen, ob Sie von diesem Problem betroffen sind, und, wenn ja, um dieses Problem zu beheben, die Workaround-/Lösungsanweisungen befolgen.

F: Handelt es sich bei diesem Problem um eine Sicherheitslücke?

Nein. Dies ist keine Sicherheitslücke, und es besteht kein Risiko für die Integrität des Produkts.

F: Ist SSH betroffen?

Nein. SSH verwendet RSA-Schlüsselpaare, aber keine Zertifikate, außer in einer seltenen Konfiguration. Damit Cisco IOS Zertifikate verwendet, muss die nächste Konfiguration vorhanden sein.

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

F: Welche festen Versionen sind für die Plattformen Classic Catalyst 2K, 3K, 4K und 6K verfügbar?

Für Polaris-basierte Plattformen (Serie 3650/3850/Catalyst 9K) ist fix ab 16.9.1 verfügbar
Für CDB-Plattform ist der Fix ab Version 15.2(7)E1a verfügbar.

Für die anderen klassischen Switching-Plattformen:

Die Commits sind in Arbeit, aber wir haben noch keine CCO-Version veröffentlicht. In der nächsten CCO-Version kann das Problem behoben werden.

Nutzen Sie für die Zwischenzeit eine der anderen verfügbaren Problemumgehungen.

F: Ist WAAS betroffen?

WAAS funktioniert weiterhin ordnungsgemäß und optimiert den Datenverkehr. AppNav-XE und die zentrale Verwaltungsschnittstelle sind jedoch offline zu dem Gerät gegangen, dessen Selbstsignaturzertifikat abgelaufen ist. Dies bedeutet, dass Sie AppNav-Cluster nicht überwachen oder keine Richtlinien für WAAS ändern können. Zusammenfassend lässt sich sagen, dass WAAS weiterhin ordnungsgemäß funktioniert, Verwaltung und Überwachung jedoch ausgesetzt werden, bis das Zertifikatproblem behoben ist. Um das Problem zu beheben, kann ein neues Zertifikat auf Cisco IOS generiert und dann in die zentrale Verwaltungsschnittstelle importiert werden.

Zugehörige Informationen

- Siehe FN70489 Problemhinweis: FN - 70489 - PKI-Selbstsigniertes Zertifikat läuft in Cisco IOS und Cisco IOS XE Software ab
- Siehe Cisco Bug-ID CSCvi48253

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.