IOS zelf-ondertekend certificaatverloop op 1 januari 2020

Inhoud

Inleiding

Dit document beschrijft de effecten en fouten die zijn veroorzaakt door het verlopen van de zelfondertekende certificaten (SSC) op Cisco-softwaresystemen, en biedt verschillende tijdelijke oplossingen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Zelfondertekende certificaten (SSC)
- Cisco IOS® versie 12.x en hoger

Gebruikte componenten

De componenten zijn de softwaresystemen die worden beïnvloed door het verstrijken van de SSC.

Alle Cisco IOS- en Cisco IOS® XE-systemen die een zelfondertekend certificaat gebruiken, die geen oplossing voor de Cisco bug-id CSCvi48253 hebben, of die geen oplossing voor de Cisco bug-id CSCvi48253 hebben toen de SSC werd gegenereerd. Dit omvat:

- Alle Cisco IOS 12.x
- Alle Cisco IOS 15.x-poorten vóór 15.6(3)M7, 15.7(3)M5, 15.8(3)M3, 15.9(3)M
- Alle Cisco IOS XE-modellen voorafgaand aan 16.9.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrond

> **Opmerking:** Dit document bevat de inhoud van FN40789 , samen met extra context, voorbeelden, updates en Q&As.

Om 00:00 op 1 januari 2020 GMT waren alle zelfondertekende certificaten (SSC) die gegenereerd waren op Cisco IOS en Cisco IOS XE systemen ingesteld op vervaldatum, tenzij het systeem een vaste versie van Cisco IOS en Cisco IOS XE gebruikte toen de SSC werd gegenereerd. Na die tijd kunnen niet-gefixeerde Cisco IOS-systemen geen nieuwe SSC's genereren. Elke dienst die zich baseert op deze zelfondertekende certificaten om een beveiligde verbinding tot stand te brengen of te beëindigen werkt niet meer na het verlopen van het certificaat.

Dit probleem heeft alleen betrekking op zelfondertekende certificaten die zijn gegenereerd door het Cisco IOS of Cisco IOS XE-apparaat en die zijn toegepast op een service op het apparaat. Certificaten die door een certificeringsinstantie (CA) zijn gegenereerd, inclusief de certificaten die door de Cisco IOS CA-functie zijn gegenereerd, worden niet beïnvloed door dit probleem.

Bepaalde functies in Cisco IOS en Cisco IOS XE-software vertrouwen op digitaal ondertekende X.509-certificaten voor validering van cryptografische identiteit. Deze certificaten worden gegenereerd door een externe CA van derden, of op het Cisco IOS of Cisco IOS XE-apparaat zelf als een zelfondertekend certificaat. Door getroffen Cisco IOS- en Cisco IOS XE-softwarereleases is de verloopdatum van het zelfondertekende certificaat ingesteld op 2020-01-01-00:00:00 UTC. Na deze datum verloopt het certificaat en is het ongeldig.

De services die kunnen vertrouwen op een zelfondertekend certificaat omvatten:

Algemene functies

- HTTP Server via TLS (HTTPS) - HTTPS veroorzaakt een fout in de browser die aangeeft dat het certificaat is verlopen.
- SSH Server - Gebruikers die X.509-certificaten gebruiken om de SSH-sessie te verifiëren, kunnen niet verifiëren. (Het gebruik van X.509-certificaten is zeldzaam. Gebruikersnaam/wachtwoordverificatie en openbare/particuliere sleutelverificatie worden niet beïnvloed.)
- RESTCONF - RESTCONF-verbindingen kunnen defect raken.

Functies voor samenwerking

- Session Initiation Protocol (SIP) via TLS
- Cisco Unified Communications Manager Express (CME) met enabled versleutelde signalering
- Cisco Unified Survivable Remote Site Telephony (SRST) met ingeschakeld versleutelde signalering
- Cisco IOS dspfarm resources (conferentie, media-afsluitpunt of transcodering) met versleutelde signalering ingeschakeld
- Skinny Client Control Protocol (SCCP) poorten voor Telephony Control Application (STCAPP) geconfigureerd met versleutelde signalering
- Media Gateway Control Protocol (MGCP) en H.323 gesprekssignalering via IP-beveiliging (IPSec) zonder een vooraf gedeelde sleutel
- Cisco Unified Communications Gateway Services API in beveiligde modus (waarvoor HTTPS wordt gebruikt)

Draadloze functies

- WAP/CAPWAP-verbindingen tussen oudere Cisco IOS-access points (gemaakt in 2005 of eerder) en draadloze LAN-controller. Zie Cisco-melding uit het veld FN63942 voor meer informatie.

Probleem

Een poging om een zelfondertekend certificaat te genereren op een getroffen Cisco IOS of Cisco IOS XE-softwarerelease na 2020-01-01-00:00:00 UTC resulteert in deze fout:

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

Diensten die afhankelijk zijn van het zelfondertekende certificaat functioneren niet. Voorbeeld:

- SIP via TLS niet voltooid.
- Apparaten die zijn geregistreerd bij Cisco Unified CME met ingeschakeld versleutelde signalering werken niet meer.
- Met Cisco Unified SRST met ingeschakeld versleutelde signalering kunnen apparaten niet worden geregistreerd.

- Cisco IOS-hostresources (conferentie, media-afsluitpunt of transcodering) met versleutelde signalering kunnen niet langer worden geregistreerd.
- STCAPP-poorten die zijn geconfigureerd met versleutelde signalering worden niet meer geregistreerd.
- Oproepen door een gateway die MGCP of H.323 vraag signalering over IPSec zonder een pre-gedeelde sleutel kan ontbreken.
- API-oproepen die de Cisco Unified Communications Gateway Services API in beveiligde modus (waarvoor HTTPS wordt gebruikt) gebruiken, kunnen mislukken.
- RESTCONF kan defect raken.
- HTTPS-sessies om het apparaat te beheren, geven een browserwaarschuwing weer, die aangeeft dat het certificaat is verlopen.
- AnyConnect SSL VPN-sessies kunnen geen ongeldig certificaat instellen of melden.
- IPsec-verbindingen kunnen niet worden gemaakt.

Hoe getroffen producten te identificeren

> **Opmerking:** Om door deze melding in het veld te worden beïnvloed, moet een apparaat een zelfondertekend certificaat hebben *en* moet het zelfondertekende certificaat worden toegepast op een of meer van de hieronder beschreven kenmerken. De aanwezigheid van een zelfondertekend certificaat alleen heeft geen invloed op de werking van het apparaat wanneer het certificaat verloopt en vereist geen onmiddellijke actie. **Om te worden geraakt, moet een inrichting voldoen aan de criteria in zowel stap 3 als stap 4 hieronder.**

Bepalen of u een zelfondertekend certificaat gebruikt:

1. Voer het show running-config | begin crypto opdracht op uw apparaat.
2. Zoek naar de crypto PKI trust-point configuratie.
3. In de crypto PKI trust-point configuratie, zoek de trust-point inschrijvingsconfiguratie. De registratie bij een vertrouwenspunt moet zo worden geconfigureerd dat er **invloed** is op "**self-signed**". Daarnaast moet ook het zelfondertekende certificaat in de configuratie verschijnen. Bericht dat de vertrouwen-punt naam niet de woorden "zelf-ondertekende"zoals aangetoond in dit volgende voorbeeld bevat.

```
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
```

   Als de trust-point inschrijving *niet* geconfigureerd is voor "selfsigned"; **het apparaat wordt NIET beïnvloed door deze melding in het veld**. Er is geen actie vereist.**Als de registratie bij een vertrouwenspunt *is* geconfigureerd voor "zelfondertekend" en als het zelfondertekende certificaat in de configuratie verschijnt**; het **apparaat kan worden beïnvloed** door deze melding in het veld. Ga verder naar stap 4.
4. Als u in Stap 3 hebt bepaald dat de registratie van vertrouwenspunten is geconfigureerd voor "zelfondertekend" en dat het zelfondertekende certificaat in de configuratie verschijnt,

controleert u of het zelfondertekende certificaat wordt toegepast op een functie op het apparaat.In deze voorbeeldconfiguraties worden verschillende functies getoond die aan de SSC kunnen worden gekoppeld:

- Voor **HTTPS Server** moet deze tekst aanwezig zijn:

```
ip http secure-server
```

Bovendien kan een vertrouwenspunt ook worden gedefinieerd zoals in het volgende codevoorbeeld. Als deze opdracht niet bestaat, wordt standaard het zelfondertekende certificaat gebruikt.

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

Als er een vertrouwenspunt is gedefinieerd en dit verwijst naar een ander certificaat dan het zelfondertekende certificaat, krijgt u geen invloed.

Voor **HTTPS Server** is het effect van het verlopen certificaat minimaal omdat zelfondertekende certificaten al niet vertrouwd zijn door webbrowsers en een waarschuwing genereren zelfs wanneer ze niet verlopen zijn. De aanwezigheid van een verlopen certificaat kan de waarschuwing die u in de browser ontvangt, wijzigen.

- Voor **SIP via TLS** is deze tekst aanwezig in het configuratiebestand:

```
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>
!
```

- Voor **Cisco Unified CME** met ingeschakeld versleutelde signalering is deze tekst aanwezig in het configuratiebestand:

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

- Voor **Cisco Unified SRST** met ingeschakeld versleutelde signalering is deze tekst aanwezig in het configuratiebestand:

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

- Voor **Cisco IOS dspfarm middel**s (Conferentie, Media-afsluitpunt of transcodering) met versleutelde signalering ingeschakeld, is deze tekst aanwezig in het configuratiebestand:

```
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>
!
```

- Voor **STCAPP-poorten** die met versleutelde signalering zijn geconfigureerd, is deze tekst aanwezig in het configuratiebestand:
```
stcapp security trust-point <self-signed-trust-point-name>
stcapp security mode encrypted
```
- Voor **Cisco Unified Communications Gateway Services API in beveiligde modus**, is deze tekst aanwezig in het configuratiebestand:
```
uc secure-wsapi
ip http secure-server
ip http secure-trust-point TP-self-signed-XXXXXXXX
```
- Voor **SSL VPN** is deze tekst in het configuratiebestand aanwezig:
```
webvpn gateway <gw name>
 ssl trust-point TP-self-signed-XXXXXXXX

OR

crypto ssl policy <policy-name>
pki trust-point <trust-point-name> sign
```
- Voor **ISAKMP en IKEv2** kan het zelfondertekende certificaat worden gebruikt als een van de configuraties aanwezig is (verdere analyse van de configuratie is vereist om te bepalen of de functie het zelfondertekende certificaat gebruikt in vergelijking met een ander certificaat):
```
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
```
- Voor **SSH Server** is het zeer onwaarschijnlijk dat u certificaten kunt gebruiken om de SSH-sessies te verifiëren. U kunt echter wel uw configuratie controleren om dit te verifiëren. Alle drie de lijnen in het volgende codevoorbeeld moeten worden weergegeven om te kunnen worden beïnvloed. **Opmerking:** Als u gebruikmaakte van gebruikersnaam en wachtwoordcombinatie naar SSH in uw apparaat dan bent u NIET getroffen.
```
ip ssh server certificate profile
 ! Certificate used by server
 server
  trust-point sign TP-self-signed-xxxxxx
```
- Voor **RESTCONF** is deze tekst aanwezig in het configuratiebestand:
```
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
```

Oplossing(en)

De oplossing is om de Cisco IOS of Cisco IOS XE-software te upgraden naar een release die de oplossing bevat:

- Cisco IOS XE-softwarerelease 16.9.1 en hoger
- Cisco IOS-softwarerelease 15.6(3)M7 en hoger; 15.7(3)M5 en hoger; of 15.8(3)M3 en hoger

Nadat u de software hebt bijgewerkt, moet u het zelfondertekende certificaat regenereren en het

exporteren naar alle apparaten die het certificaat kunnen vereisen in hun vertrouwenswinkel.

Er zijn drie tijdelijke oplossingen beschikbaar als een onmiddellijke software-upgrade niet mogelijk is:

1. Een geldig certificaat verkrijgen van een certificeringsinstantie van het derde deel (CA).
2. Gebruik de Cisco IOS CA Server om een nieuw certificaat te genereren.
3. Gebruik OpenSSL om een nieuw zelfondertekend certificaat te genereren.

1. Een geldig certificaat verkrijgen van een certificeringsinstantie van een derde partij (CA)

Installeer een certificaat van een certificeringsinstantie. Gemeenschappelijke CA's omvatten: Comodo Let's Encrypt, RapidSSL, Thawte, Sectigo, GeoTrust, Symantec, enzovoort. Met deze tijdelijke oplossing wordt een certificaatverzoek gegenereerd en weergegeven door Cisco IOS. De beheerder kopieert vervolgens het verzoek, legt het voor aan een derde CA, en haalt het resultaat terug.

> **Opmerking:** Het gebruik van een CA voor het ondertekenen van certificaten wordt beschouwd als best practice voor de beveiliging. Deze procedure wordt in deze melding als tijdelijke oplossing geboden; het is echter beter om het door CA ondertekende certificaat van derden te blijven gebruiken nadat u deze tijdelijke oplossing hebt toegepast, in plaats van een zelfondertekend certificaat te gebruiken.

U installeert een certificaat van een externe CA als volgt:

1. Een aanvraag voor certificaatondertekening maken (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. De MVO voorleggen aan de derde CA.**Opmerking:** De procedure om de CSR aan een derde CA voor te leggen en het certificaat op te halen dat resulteert, varieert afhankelijk van de gebruikte CA. Raadpleeg de documentatie bij uw CA voor instructies over hoe u deze stap moet uitvoeren.
2. Download het nieuwe identiteitscertificaat voor de router samen met het CA-certificaat.
3. Installeer het CA-certificaat op het apparaat:

```
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. Installeer het identiteitscertificaat op het apparaat:

```
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. Gebruik de Cisco IOS CA-server om een nieuw certificaat te genereren

Gebruik de lokale server van de Cisco IOS-certificeringsinstantie om een nieuw certificaat te genereren en te ondertekenen.

Opmerking:de lokale CA-serverfunctie is niet voor alle producten beschikbaar.

```
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. Gebruik OpenSSL om een nieuw zelfondertekend certificaat te genereren

Gebruik OpenSSL om een PKCS 12-certificaatbundel te genereren en de bundel te importeren naar Cisco IOS.

LINUX, UNIX of MAC (OSX) Voorbeeld

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 of Cisco IOS XE-routervoorbeeld

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
```

Controleer of het nieuwe certificaat is geïnstalleerd:

```
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
```

Opmerking: Zelfondertekende certificaten verlopen op 00:00 1 januari 2020 UTC en u kunt ze na die tijd niet meer maken.

Vraag en antwoord

V: Waar gaat het om?

Zelfondertekende X.509 PKI-certificaten die zijn gegenereerd op producten waarop Cisco IOS- of Cisco IOS XE-versies worden uitgevoerd, verlopen op 1 januari 2020, 10.00 uur en 20 minuten. Nieuwe zelfondertekende certificaten kunnen niet worden aangemaakt op getroffen apparaten na 01/01/2020 00:00:00 UTC. Elke dienst die zich baseert op deze zelfondertekende certificaten kan niet meer werken nadat het certificaat is verlopen.

V: Wat is de impact op een clientnetwerk als een zelfondertekend certificaat verloopt voor hun product?

De functionaliteit van een beïnvloed product dat afhankelijk is van de zelfondertekende certificaten kan niet meer werken nadat het certificaat is verlopen. Raadpleeg de melding uit het veld voor meer informatie.

V: Hoe weet ik of deze kwestie mij aangaat?

De melding uit het veld bevat instructies om te bepalen of u een zelfondertekend certificaat gebruikt en of uw configuratie door dit probleem wordt beïnvloed. Raadpleeg de sectie "Hoe getroffen producten te identificeren" in de melding uit het veld.

V: Is er een script dat ik kan draaien om te zien of ik beïnvloed ben?

Ja. Gebruik Cisco CLI Analyzer, voer een System Diagnostic Run uit. Indien het certificaat aanwezig is en wordt gebruikt, kan een signalering worden getoond. https://cway.cisco.com/cli/

V. Heeft Cisco softwareoplossingen voor dit probleem geleverd?

Ja. Cisco heeft softwareoplossingen voor dit probleem en tijdelijke oplossingen vrijgegeven voor het geval dat een software-upgrade niet onmiddellijk uitvoerbaar is. Raadpleeg de melding uit het

veld voor meer informatie.

V: Heeft deze kwestie invloed op elk Cisco-product dat een certificaat gebruikt?

Nee. Dit probleem heeft **alleen** betrekking op **producten die zelfondertekende certificaten gebruiken die zijn gegenereerd door specifieke versies van Cisco IOS of Cisco IOS XE** met het certificaat dat is toegepast op een service op het product. Producten die gebruikmaken van certificaten die zijn gegenereerd door een certificeringsinstantie (CA) worden niet beïnvloed door dit probleem.

V: Gebruiken Cisco-producten alleen zelfondertekende certificaten?

Nee. Certificaten kunnen worden gegenereerd door een externe certificeringsinstantie van een derde partij of op het Cisco IOS of Cisco IOS XE-apparaat zelf als een zelfondertekend certificaat. Specifieke gebruikerseisen kunnen het gebruik van zelfondertekende certificaten vereisen. Certificaten gegenereerd door een certificeringsinstantie (CA) worden niet beïnvloed door dit probleem.

V. Waarom is dit probleem opgetreden?

Helaas, ondanks de beste inspanningen van technologieverkopers, doen zich nog steeds softwaredefecten voor. Wanneer een bug in een Cisco-technologie wordt ontdekt, engageren we ons voor transparantie en om onze gebruikers de informatie te geven die ze nodig hebben om hun netwerk te beschermen.

In dit geval wordt het probleem veroorzaakt door een bekend softwarebug waarin getroffen versies van Cisco IOS en Cisco IOS XE de verloopdatum van het zelfondertekende certificaat altijd kunnen instellen op 01/01/2020-00:00:00 UTC. Na deze datum verloopt het certificaat en is het ongeldig, wat gevolgen kan hebben voor de productfunctionaliteit.

V: Waarom is gekozen voor een verloopdatum van 1 januari 2020, 00:00 UTC?

Certificaten hebben doorgaans een verloopdatum. In het geval van deze softwarebug wordt de datum 1 januari 2020 meer dan 10 jaar geleden gebruikt tijdens de ontwikkeling van de Cisco IOS- en Cisco IOS XE-software en is dit een menselijke fout.

V: Welke producten vallen onder deze kwestie?

Alle Cisco-producten waarop Cisco IOS-releases worden uitgevoerd voorafgaand aan 15.6(3)M07, 15.7(3)M05, 15.8(3)M03 en 15.9(3)M en alle Cisco-producten die Cisco IOS XE releases voorafgaand aan 16.9.1 uitvoeren

V: Wat moeten gebruikers doen?

U moet de melding uit het veld bekijken om te beoordelen of dit probleem voor u gevolgen heeft en, indien dit het geval is, de instructies van de tijdelijke oplossing/oplossing volgen om dit probleem te verhelpen.

V: Is deze kwestie een veiligheidskwetsbaarheid?

Nee. Dit is geen beveiligingskwetsbaarheid en er is geen risico voor de integriteit van het product.

V: Wordt SSH beïnvloed?

Nr. SSH gebruikt geen RSA-sleutelparen, maar gebruikt geen certificaten behalve in een zeldzame configuratie. Cisco IOS kan certificaten alleen gebruiken als de volgende configuratie aanwezig is.

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

V: Welke vaste versies zijn beschikbaar voor de Classic Catalyst 2K, 3K, 4K, 6K platforms?

Voor Polaris-gebaseerde platforms (3650/3850/Catalyst 9K-serie) is fix beschikbaar vanaf 16.9.1
Voor CDB platform is fix beschikbaar vanaf 15.2(7)E1a

Voor de andere Classic Switching Platforms:

Er wordt gewerkt aan vastleggingen, maar we hebben geen CCO release geplaatst. Volgende CCO release kan de fix hebben.

Maak in de tussentijd gebruik van een van de andere beschikbare tijdelijke oplossingen.

V: Wordt WAAS aangetast?

WAAS blijft correct werken en het verkeer optimaliseren, maar AppNav-XE & de Central Manager gingen offline naar het apparaat dat een verlopen zelfondertekend certificaat heeft. Dit betekent dat u AppNav-Cluster niet kunt controleren en geen beleid voor WAAS kunt wijzigen. Samengevat, blijft WAAS behoorlijk werken, maar het beheer en de controle worden opgeschort tot het certificaatprobleem wordt opgelost. Om het probleem op te lossen moet er een nieuw certificaat worden gegenereerd op Cisco IOS en vervolgens worden geïmporteerd in de Central Manager.

Gerelateerde informatie

- Zie FN70489 melding uit het veld: FN - 70489 - Vervaldatum van PKI-zelfondertekend certificaat in Cisco IOS en Cisco IOS XE-software
- Zie Cisco bug-id CSCvi48253

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.