Expiration du certificat autosigné IOS le 1er janvier 2020

Contenu

Introduction

Ce document décrit les effets et les erreurs provoqués par l'expiration des certificats auto-signés (SSC) sur les systèmes logiciels Cisco, et fournit diverses solutions de contournement.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Certificats auto-signés (SSC)
- Cisco IOS® versions 12.x et ultérieures

Components Used

Les composants sont les systèmes logiciels concernés par l'expiration du SSC.

Tous les systèmes Cisco IOS et Cisco IOS® XE qui utilisent un certificat auto-signé, qui n'ont pas l'ID de bogue Cisco CSCvi48253 fix, ou qui n'ont pas l'ID de bogue Cisco CSCvi48253 fix quand le SSC a été généré. Cela inclut :

- Tout Cisco IOS 12.x
- Toutes les versions de Cisco IOS 15.x antérieures à 15.6(3)M7, 15.7(3)M5, 15.8(3)M3, 15.9(3)M
- Toutes les versions de Cisco IOS XE antérieures à 16.9.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Fond

> **Note**: Ce document contient le contenu de FN40789, ainsi que le contexte supplémentaire, des exemples, des mises à jour et des questions-réponses.

À00:00 le 1er janvier 2020 UTC, tous les certificats auto-signés (SSC) générés sur les systèmes Cisco IOS et Cisco IOS XE étaient configurés pour expirer, sauf si le système exécutait une version fixe de Cisco IOS et Cisco IOS XE lors de la génération du SSC. Au-delà de ce délai, les systèmes Cisco IOS non réparés ne peuvent plus générer de nouvelles SSC. Tout service qui s'appuie sur ces certificats auto-signés pour établir ou mettre fin à une connexion sécurisée ne fonctionne pas après l'expiration du certificat.

Ce problème concerne uniquement les certificats auto-signés qui ont été générés par le périphérique Cisco IOS ou Cisco IOS XE et appliqués à un service sur le périphérique. Les certificats qui ont été générés par une autorité de certification (CA), qui inclut les certificats générés par la fonctionnalité CA de Cisco IOS, ne sont pas affectés par ce problème.

Certaines fonctionnalités des logiciels Cisco IOS et Cisco IOS XE reposent sur des certificats X.509 signés numériquement pour la validation de l'identité cryptographique. Ces certificats sont soit générés par une autorité de certification externe, soit sur le périphérique Cisco IOS ou Cisco IOS XE lui-même en tant que certificat auto-signé. Les versions de Cisco IOS et de Cisco IOS XE affectées définissent la date d'expiration du certificat auto-signé sur 2020-01-01 00:00:00 UTC. Après cette date, le certificat expire et n'est plus valide.

Les services pouvant s'appuyer sur un certificat auto-signé sont les suivants :

Caractéristiques générales

- HTTP Server over TLS (HTTPS) : HTTPS génère une erreur dans le navigateur qui indique que le certificat a expiré.
- Serveur SSH : les utilisateurs qui utilisent des certificats X.509 pour authentifier la session SSH peuvent ne pas s'authentifier. (L'utilisation de certificats X.509 est rare. Les authentifications par nom d'utilisateur/mot de passe et par clé publique/privée ne sont pas affectées.)
- RESTCONF : les connexions RESTCONF peuvent échouer.

Fonctionnalités de collaboration

- Protocole SIP (Session Initiation Protocol) sur TLS
- Cisco Unified Communications Manager Express (CME) avec signalisation cryptée activée
- Cisco Unified Survivable Remote Site Telephony (SRST) avec signalisation cryptée activée
- Cisco IOS dspfarm ressources (conférence, point de terminaison média ou transcodage) avec signalisation cryptée activée
- Ports Skinny Client Control Protocol (SCCP) Telephony Control Application (STCAPP) configurés avec signalisation chiffrée
- Protocole MGCP (Media Gateway Control Protocol) et signalisation d'appel H.323 sur sécurité IP (IPSec) sans clé prépartagée
- API Cisco Unified Communications Gateway Services en mode sécurisé (utilisant HTTPS)

Fonctionnalités sans fil

- Connexions LWAPP/CAPWAP entre les anciens points d'accès Cisco IOS (fabriqués en 2005 ou avant) et le contrôleur LAN sans fil. Pour plus d'informations, reportez-vous à la note de service Cisco FN63942.

Problème

Une tentative de génération d'un certificat auto-signé sur une version du logiciel Cisco IOS ou Cisco IOS XE affectée après 2020-01-01 00:00:00 UTC entraîne cette erreur :

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

Les services qui reposent sur le certificat auto-signé ne fonctionnent pas. Exemple :

- Les appels SIP sur TLS ne sont pas terminés.
- Les périphériques enregistrés auprès de Cisco Unified CME avec signalisation cryptée activée ne fonctionnent plus.
- Cisco Unified SRST avec signalisation chiffrée activée ne permet pas aux périphériques de s'enregistrer.
- Les ressources Cisco IOS dspfarm (conférence, point de terminaison média ou transcodage) avec signalisation chiffrée activée ne sont plus enregistrées.

- Les ports STCAPP configurés avec la signalisation chiffrée ne sont plus enregistrés.
- Les appels passant par une passerelle que MGCP ou H.323 signalent via IPSec sans clé pré-partagée peuvent échouer.
- Les appels d'API qui utilisent l'API Cisco Unified Communications Gateway Services en mode sécurisé (qui utilisent HTTPS) peuvent échouer.
- RESTCONF peut échouer.
- Les sessions HTTPS de gestion du périphérique affichent un avertissement du navigateur, qui indique que le certificat a expiré.
- Les sessions VPN SSL AnyConnect ne parviennent pas à établir ou à signaler un certificat non valide.
- Les connexions IPSec peuvent ne pas être établies.

Comment identifier les produits affectés

> **Note**: Pour être affecté par cette notification de champ, un périphérique doit avoir un certificat auto-signé défini *et* le certificat auto-signé doit être appliqué à une ou plusieurs fonctionnalités comme indiqué ci-dessous. La présence d'un certificat auto-signé seul n'a pas d'impact sur le fonctionnement du périphérique lorsque le certificat expire et ne nécessite pas d'action immédiate. **Pour être affecté, un périphérique doit répondre aux critères des étapes 3 et 4 ci-dessous.**

Pour déterminer si vous utilisez un certificat auto-signé :

1. Saisissez le show running-config | begin crypto sur votre périphérique.
2. Recherchez la configuration du point de confiance PKI de chiffrement.
3. Dans la configuration du point de confiance PKI de chiffrement, recherchez la configuration d'inscription du point de confiance. L'inscription du point de confiance doit être configurée pour que l'**« auto-signé** » soit affecté. En outre, le certificat auto-signé doit également apparaître dans la configuration. Notez que le nom du point de confiance ne contient pas les mots « self-signed » (auto-signé), comme indiqué dans l'exemple suivant.

```
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
```

   Si l'inscription du point de confiance n'est *pas* **configurée pour** « auto-signé » ; **le périphérique n'est PAS affecté par cet avis de champ**. Aucune action n'est requise.**Si l'inscription du point de confiance** *est* **configurée pour « auto-signé » et si le certificat auto-signé apparaît dans la configuration** ; le **périphérique peut être affecté** par cet avis de champ. Passez à l'étape 4.
4. Si vous avez déterminé à l'étape 3 que l'inscription de point de confiance est configurée pour « auto-signé » et que le certificat auto-signé apparaît dans la configuration, vérifiez si le certificat auto-signé est appliqué à une fonctionnalité du périphérique.Diverses fonctions pouvant être associées à la carte SSC sont présentées dans ces exemples de configuration :

- Pour le **serveur HTTPS**, ce texte doit être présent :

```
ip http secure-server
```

En outre, un point de confiance peut également être défini comme indiqué dans l'exemple de code suivant. Si cette commande n'est pas présente, le comportement par défaut consiste à utiliser le certificat auto-signé.

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

Si un point de confiance est défini et qu'il pointe vers un certificat autre que le certificat auto-signé, vous n'êtes pas affecté.

Pour le **serveur HTTPS**, l'impact du certificat expiré est mineur car les certificats auto-signés ne sont déjà pas approuvés par les navigateurs Web et génèrent un avertissement même lorsqu'ils ne sont pas expirés. La présence d'un certificat expiré peut modifier l'avertissement que vous recevez dans le navigateur.

- Pour **SIP sur TLS**, ce texte est présent dans le fichier de configuration :

```
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>
!
```

- Pour **Cisco Unified CME** avec la signalisation chiffrée activée, ce texte est présent dans le fichier de configuration :

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

- Pour **Cisco Unified SRST** avec la signalisation chiffrée activée, ce texte est présent dans le fichier de configuration :

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

- Pour **Cisco IOS dspfarm ressource**s (Conference, Media Termination Point ou Transcoding) avec la signalisation chiffrée activée, ce texte est présent dans le fichier de configuration :

```
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>
!
```

- Pour les **ports STCAPP** configurés avec la signalisation chiffrée, ce texte est présent dans le fichier de configuration :
```
stcapp security trust-point <self-signed-trust-point-name>
stcapp security mode encrypted
```
- Pour l'**API des services Cisco Unified Communications Gateway en mode sécurisé**, ce texte est présent dans le fichier de configuration :
```
uc secure-wsapi
ip http secure-server
ip http secure-trust-point TP-self-signed-XXXXXXXX
```
- Pour **SSLVPN**, ce texte est présent dans le fichier de configuration :
```
webvpn gateway <gw name>
 ssl trust-point TP-self-signed-XXXXXXXX

OR

crypto ssl policy <policy-name>
pki trust-point <trust-point-name> sign
```
- Pour **ISAKMP et IKEv2**, le certificat auto-signé peut être utilisé si l'une des configurations est présente (une analyse plus approfondie de la configuration est requise afin de déterminer si la fonctionnalité utilise le certificat auto-signé par rapport à un autre certificat) :
```
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
```
- Pour **SSH Server**, il est extrêmement peu probable que vous puissiez utiliser des certificats pour authentifier les sessions SSH. Cependant, vous pouvez vérifier votre configuration pour ce faire. Vous devez afficher les trois lignes dans l'exemple de code suivant pour être affecté. **Note**: Si vous avez utilisé la combinaison nom d'utilisateur/mot de passe pour SSH sur votre périphérique, vous n'êtes PAS affecté.
```
ip ssh server certificate profile
 ! Certificate used by server
 server
  trust-point sign TP-self-signed-xxxxxx
```
- Pour **RESTCONF**, ce texte est présent dans le fichier de configuration :
```
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
```

Solution(s)

La solution consiste à mettre à niveau le logiciel Cisco IOS ou Cisco IOS XE vers une version qui inclut le correctif :

- Logiciel Cisco IOS XE versions 16.9.1 et ultérieures
- Logiciel Cisco IOS version 15.6(3)M7 et ultérieure ; 15.7(3)M5 et ultérieures ; ou 15.8(3)M3 et versions ultérieures

Après avoir mis à niveau le logiciel, vous devez régénérer le certificat auto-signé et l'exporter vers tous les périphériques qui peuvent exiger le certificat dans leur magasin de confiance.

Trois solutions de contournement sont disponibles si une mise à niveau logicielle immédiate n'est

pas possible :

1. Obtenez un certificat valide auprès d'une autorité de certification (CA) tierce partie.
2. Utilisez le serveur Cisco IOS CA Server pour générer un nouveau certificat.
3. Utilisez OpenSSL pour générer un nouveau certificat auto-signé.

1. Obtenir un certificat valide auprès d'une autorité de certification tierce

Installer un certificat d'une autorité de certification. Les AC courantes incluent : Comodo, Let's Encrypt, RapidSSL, Thawte, Sectigo, GeoTrust, Symantec, etc. Avec cette solution, une demande de certificat est générée et affichée par Cisco IOS. L'administrateur copie ensuite la demande, l'envoie à une autorité de certification tierce et récupère le résultat.

> **Note**: L'utilisation d'une autorité de certification pour signer des certificats est considérée comme une meilleure pratique de sécurité. Cette procédure est fournie à titre de solution de contournement dans cet avis de champ ; toutefois, il est préférable de continuer à utiliser le certificat signé par une autorité de certification tierce après avoir appliqué cette solution de contournement, plutôt que d'utiliser un certificat auto-signé.

Pour installer un certificat d'une autorité de certification tierce :

1. Créer une demande de signature de certificat (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. Envoyez le CSR à l'autorité de certification tierce.**Note**: La procédure d'envoi du CSR à une autorité de certification tierce et de récupération du certificat dont les résultats varient en fonction de l'autorité de certification utilisée. Consultez la documentation de votre autorité de certification pour savoir comment effectuer cette étape.
2. Téléchargez le nouveau certificat d'identité du routeur avec le certificat CA.
3. Installez le certificat CA sur le périphérique :

```
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. Installez le certificat d'identité sur le périphérique :

```
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. Utilisez le serveur Cisco IOS CA pour générer un nouveau certificat

Utilisez le serveur Cisco IOS Certificate Authority local pour générer et signer un nouveau certificat.

Remarque : la fonctionnalité de serveur AC local n'est pas disponible sur tous les produits.

```
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. Utiliser OpenSSL pour générer un nouveau certificat auto-signé

Utilisez OpenSSL pour générer un lot de certificats PKCS12 et importer le lot dans Cisco IOS.

Exemple LINUX, UNIX ou 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
```

Exemple de routeur Cisco IOS ou Cisco IOS XE

```
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
```

Vérifiez que le nouveau certificat est installé :

```
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
```

> **Note**: Les certificats auto-signés expirent le 1er janvier 2020 à 00:00 UTC et vous ne pourrez plus les créer après cette date.

Q&R

Q : Quel est le problème ?

Les certificats PKI X.509 auto-signés générés sur les produits qui exécutent les versions affectées de Cisco IOS ou Cisco IOS XE expirent le 01/01/2020 00:00:00 UTC. Impossible de créer de nouveaux certificats auto-signés sur les périphériques concernés après le 01/01/2020 00:00:00 UTC. Tout service qui s'appuie sur ces certificats auto-signés ne peut plus fonctionner après l'expiration du certificat.

Q : Quel est l'impact sur un réseau client si un certificat auto-signé expire pour son produit ?

Les fonctionnalités des produits concernés qui reposent sur les certificats auto-signés ne peuvent plus fonctionner après l'expiration du certificat. Pour plus d'informations, reportez-vous à l'avis relatif aux champs.

Q : Comment savoir si je suis concerné par ce problème ?

La notice de champ fournit des instructions pour déterminer si vous utilisez un certificat auto-signé et si votre configuration est affectée par ce problème. Reportez-vous à la section « Identification des produits affectés » de la notice de service.

Q : Y a-t-il un script que je puisse exécuter pour voir si je suis affecté ?

Oui. Utilisez Cisco CLI Analyzer, exécutez un diagnostic du système. Si le certificat est présent et qu'il est utilisé, une alerte peut être affichée. https://cway.cisco.com/cli/

Q. Cisco a-t-il fourni des correctifs logiciels pour ce problème ?

Oui. Cisco a publié des correctifs logiciels pour ce problème ainsi que des solutions de contournement dans le cas où une mise à niveau logicielle ne serait pas immédiatement possible. Veuillez consulter la notice de champ pour plus de détails.

Q : Ce problème affecte-t-il les produits Cisco qui utilisent un certificat ?

Non. Ce problème concerne **uniquement les produits qui utilisent des certificats auto-signés générés par des versions spécifiques de Cisco IOS ou de Cisco IOS XE** avec le certificat appliqué

à un service sur le produit. Les produits qui utilisent des certificats générés par une autorité de certification (CA) ne sont pas affectés par ce problème.

Q : Les produits Cisco utilisent-ils uniquement des certificats auto-signés ?

Non. Les certificats peuvent être générés par une autorité de certification tierce externe ou sur le périphérique Cisco IOS ou Cisco IOS XE lui-même en tant que certificat auto-signé. Des exigences utilisateur spécifiques peuvent nécessiter l'utilisation de certificats auto-signés. Les certificats générés par une autorité de certification ne sont pas affectés par ce problème.

Q. Pourquoi ce problème s'est-il produit ?

Malheureusement, malgré tous les efforts des fournisseurs de technologie, des défauts logiciels persistent. Lorsqu'un bogue est détecté dans une technologie Cisco, nous nous engageons à la transparence et à fournir à nos utilisateurs les informations dont ils ont besoin pour protéger leur réseau.

Dans ce cas, le problème est causé par un bogue logiciel connu dans lequel les versions affectées de Cisco IOS et de Cisco IOS XE peuvent toujours définir la date d'expiration du certificat auto-signé sur 01/01/2020 00:00:00 UTC. Après cette date, le certificat expire et n'est plus valide, ce qui peut avoir un impact sur les fonctionnalités du produit.

Q : Pourquoi a-t-on choisi une date d'expiration du 1er janvier 2020 00:00:00 UTC ?

Les certificats ont généralement une date d'expiration. Dans le cas de ce bogue logiciel, la date du 1er janvier 2020 a été utilisée lors du développement des logiciels Cisco IOS et Cisco IOS XE il y a plus de 10 ans et constitue une erreur humaine.

Q : Quels produits sont concernés par ce problème ?

Tout produit Cisco qui exécute des versions de Cisco IOS antérieures à 15.6(03)M07, 15.7(03)M05, 15.8(03)M03 et 15.9(03)M et tout produit Cisco qui exécute des versions de Cisco IOS XE antérieures à 16.9.1

Q : Que doivent faire les utilisateurs ?

Vous devez consulter l'avis sur site pour déterminer si vous êtes concerné par ce problème et, si tel est le cas, suivre les instructions de la solution de contournement/de la solution pour atténuer ce problème.

Q : Ce problème est-il une faille de sécurité ?

Non. Il ne s'agit pas d'une faille de sécurité et l'intégrité du produit n'est pas compromise.

Q : SSH est-il affecté ?

Non. SSH utilise des paires de clés RSA, mais pas de certificats, sauf dans une configuration rare. Pour que Cisco IOS utilise des certificats, la configuration suivante doit être présente.

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

Q : Quelles sont les versions fixes disponibles pour les plates-formes Catalyst classiques 2K, 3K, 4K, 6K ?

Pour les plates-formes basées sur Polaris (série 3650/3850/Catalyst 9K), le correctif est disponible à partir de la version 16.9.1
Pour la plate-forme CDB, le correctif est disponible à partir de la version 15.2(7)E1a

Pour les autres plates-formes de commutation classiques :

Les engagements sont en cours, mais nous n'avons pas publié la version CCO. La prochaine version de CCO peut être corrigée.

Dans l'intervalle, veuillez utiliser l'une des autres solutions de contournement disponibles.

Q : WAAS est-il affecté ?

WAAS continue de fonctionner correctement et d'optimiser le trafic. Cependant, AppNav-XE et le Gestionnaire central se sont déconnectés du périphérique dont le certificat auto-signé a expiré. Cela signifie que vous ne pouvez pas surveiller AppNav-Cluster ou modifier les stratégies pour WAAS. En résumé, WAAS continue de fonctionner correctement, mais la gestion et la surveillance sont suspendues jusqu'à ce que le problème de certificat soit résolu. Pour résoudre le problème, un nouveau certificat peut être généré sur Cisco IOS, puis importé dans le Gestionnaire central.

Informations connexes

- Voir FN70489 Field Notice : FN - 70489 - Expiration du certificat autosigné PKI dans les logiciels Cisco IOS et Cisco IOS XE
- Voir ID de bogue Cisco CSCvi48253

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.