2020年1月1日のIOS自己署名証明書の有効期限

内容

概要

このドキュメントでは、シスコソフトウェアシステムでの自己署名証明書(SSC)の期限切れによる影響とエラーについて説明し、さまざまな回避策を提供します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 自己署名証明書(SSC)
- Cisco IOS®バージョン12.x以降

使用するコンポーネント

これらのコンポーネントは、SSCの有効期限の影響を受けるソフトウェアシステムです。

自己署名証明書を使用するすべてのCisco IOSシステムおよびCisco IOS® XEシステム。Cisco Bug ID CSCvi48253 の修正が含まれていないか、SSCの生成時にCisco Bug ID CSCvi48253 の修正が含まれていないものです。これには、次のような特徴があります。

- すべてのCisco IOS 12.x
- 15.6(3)M7、15.7(3)M5、15.8(3)M3、15.9(3)Mより前のすべてのCisco IOS 15.x
- 16.9.1より前のすべてのCisco IOS XE

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景

> **注**：このドキュメントには、FN40789 の内容に加え、追加のコンテキスト、例、アップデート、およびQ&Aが含まれています。

2020年1月1日(UTC)の00:00に、Cisco IOSおよびCisco IOS XEシステムで生成されたすべての自己署名証明書(SSC)は、SSCの生成時にシステムでCisco IOSおよびCisco IOS XEの修正バージョンが実行されていた場合を除き、期限が切れるように設定されました。その後、固定されていないCisco IOSシステムは新しいSSCを生成できません。これらの自己署名証明書に依存してセキュアな接続を確立または終了するサービスは、証明書の有効期限が切れた後は機能しません。

この問題に該当するのは、Cisco IOSまたはCisco IOS XEデバイスによって生成され、デバイス上のサービスに適用された自己署名証明書だけです。Cisco IOS CA機能によって生成された証明書を含む、認証局(CA)によって生成された証明書は、この問題の影響を受けません。

Cisco IOSおよびCisco IOS XEソフトウェアの特定の機能は、デジタル署名されたX.509証明書を使用して暗号化IDを検証します。これらの証明書は、外部サードパーティCAによって生成されるか、Cisco IOSまたはCisco IOS XEデバイス自体で自己署名証明書として生成されます。該当するCisco IOSおよびCisco IOS XEソフトウェアリリースでは、自己署名証明書の有効期限が2020-01-01 00:00:00 UTCに設定されています。この日付を過ぎると、証明書は期限切れになり、無効になります。

自己署名証明書に依存できるサービスには、次のものがあります。

一般的な機能

- HTTP Server over TLS(HTTPS):HTTPSは、証明書が期限切れであることを示すエラーをブラウザで生成します。
- SSHサーバ：SSHセッションの認証にX.509証明書を使用するユーザは、認証に失敗する可能性があります。(X.509証明書の使用はまれです。ユーザ名/パスワード認証と公開/秘密キー認証は影響を受けません)。
- RESTCONF:RESTCONF接続が失敗する可能性があります。

コラボレーション機能

- Session Initiation Protocol(SIP)over TLS
- Cisco Unified Communications Manager Express(CME)（暗号化シグナリングが有効）
- 暗号化シグナリングが有効なCisco Unified Survivable Remote Site Telephony(SRST)
- Cisco IOS dspfarm リソース（会議、メディアターミネーションポイント、またはトランスコーディング）と暗号化シグナリングの有効化
- 暗号化されたシグナリングで設定されたSkinny Client Control Protocol(SCCP)Telephony Control Application(STCAPP)ポート
- 事前共有キーを使用しないMedia Gateway Control Protocol(MGCP)およびH.323 Call Signaling over IP Security(IPSec)
- セキュアモードのCisco Unified Communications Gateway Services API（HTTPSを使用）

ワイヤレス機能

- 古いCisco IOSアクセスポイント（2005年以前に製造）とワイヤレスLANコントローラ間のLWAPP/CAPWAP接続。詳細については、Cisco Field Notice FN63942を参照してください。

問題

2020-01-01 00:00:00 UTC以降の該当するCisco IOSまたはCisco IOS XEソフトウェアリリースで自己署名証明書(SSC)を生成しようとすると、次のエラーが発生します。

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

自己署名証明書に依存するサービスは機能しません。以下に、いくつかの例を示します。

- SIP over TLSコールが完了しません。
- 暗号化シグナリングが有効なCisco Unified CMEに登録されたデバイスは機能しなくなります。
- 暗号化シグナリングが有効なCisco Unified SRSTでは、デバイスの登録が許可されません。
- 暗号化シグナリングが有効になっているCisco IOS dspfarmリソース（会議、メディアターミネーションポイント、またはトランスコーディング）が登録されなくなりました。
- 暗号化シグナリングで設定されたSTCAPPポートが登録されなくなりました。
- 事前共有キーを使用せずにMGCPまたはH.323コールシグナリングをIPSec経由で行うゲートウェイ経由のコールは、失敗する可能性があります。
- セキュアモード（HTTPSを使用）でCisco Unified Communications Gateway Services APIを使用するAPIコールは失敗する可能性があります。
- RESTCONFは失敗する可能性があります。
- デバイスを管理するHTTPSセッションでは、証明書の有効期限が切れたことを示すブラウザ

の警告が表示されます。
- AnyConnect SSL VPNセッションが無効な証明書を確立または報告できない。
- IPSec接続の確立が失敗する可能性があります。

該当製品の識別方法

注：このField Noticeの影響を受けるには、デバイスに自己署名証明書が定義されていると、*自己署名証明書が次に示す1つ以上の機能に適用されている必要があります*。自己署名証明書が存在するだけでは、証明書の有効期限が切れた場合のデバイスの動作に影響せず、ただちにアクションを実行する必要はありません。**デバイスが影響を受けるには、次のステップ3とステップ4の両方の基準を満たしている必要があります。**

自己署名証明書を使用しているかどうかを確認するには、次の手順を実行します。

1. 次を入力します。 show running-config | begin crypto コマンドを使用します。
2. クリプトPKIトラストポイント設定を探します。
3. crypto PKIトラストポイント設定で、トラストポイント登録設定を探します。トラストポイント登録は、「**自己署名**」が影響を受けるように設定する必要があります。また、自己署名証明書も設定に表示される必要があります。次の例に示すように、トラストポイント名に「self-signed」という単語が含まれていないことに注意してください。

```
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
```

トラストポイント登録が「自己署名」**に対して***設定されていない***場合、デバイスはこのField Noticeの影響を受けません。**必要な操作はありません。トラストポイント登録が**「自己署名」用に設定され、自己署名証明書が設定に表示される場合は**、このField Noti**ceがデバイスに影響を与える可能性があります。**ステップ 4 に進みます。
4. ステップ3で、トラストポイント登録が「自己署名」用に設定され、自己署名証明書が設定に表示されると判断した場合は、自己署名証明書がデバイスの機能に適用されているかどうかを確認します。SSCに関連付けることができる各種機能を次の設定例に示します。

- **HTTPSサーバ**の場合、次のテキストが必要です。

```
ip http secure-server
```

また、次のコード例に示すように、トラストポイントを定義することもできます。このコマンドが存在しない場合、デフォルトの動作では自己署名証明書が使用されます。

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

トラストポイントが定義され、自己署名証明書とは異なる証明書を指している場合は、影響を受けません。

HTTPSサーバの場合、自己署名証明書はすでにWebブラウザで信頼されていないため、期限切れの証明書の影響はわずかです。自己署名証明書が期限切れでない場合でも、警告が生成されます。期限切れの証明書が存在すると、ブラウザに表示される警告が変わる場合があります。

- SIP over TLSの場合、設定ファイルには次のテキストが含まれます。

```
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>
!
```

- 暗号化シグナリングが有効になっているCisco Unified CMEの場合、コンフィギュレーションファイルには次のテキストが含まれています。

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

- 暗号化シグナリングが有効になっているCisco Unified SRSTの場合、コンフィギュレーションファイルには次のテキストが含まれています。

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

- を参照 Cisco IOS dspfarm リソース（会議、メディアターミネーションポイント、またはトランスコーディング）で暗号化シグナリングが有効になっている場合、次のテキストがコンフィギュレーションファイルに存在します。

```
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>
!
```

- 暗号化されたシグナリングが設定されたSTCAPPポートの場合、コンフィギュレーションファイルには次のテキストが存在します。

```
stcapp security trust-point <self-signed-trust-point-name>
stcapp security mode encrypted
```

- セキュアモードのCisco Unified Communications Gateway Services APIの場合、コンフィギュレーションファイルには次のテキストが含まれています。

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

- SSLVPNの場合、コンフィギュレーションファイルには次のテキストが含まれています。

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

OR
```

```
crypto ssl policy <policy-name>
pki trust-point <trust-point-name> sign
```

- **ISAKMPおよびIKEv2**の場合、いずれかの設定が存在すれば自己署名証明書を使用できます（この機能で自己署名証明書を使用するのか、別の証明書を使用するのかを判断するには、設定をさらに分析する必要があります）。

```
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
```

- **SSHサーバ**の場合、証明書を使用してSSHセッションを認証することはほとんどありません。ただし、設定を確認して確認できます。次のコード例に示す3つの行すべてに影響を与える必要があります。 **注：**ユーザ名とパスワードの組み合わせを利用してデバイスにSSH接続しても、影響はありません。

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

- **RESTCONF**の場合、設定ファイルには次のテキストが含まれます。

```
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
```

解決策

解決策は、Cisco IOSまたはCisco IOS XEソフトウェアを、次の修正を含むリリースにアップグレードすることです。

- Cisco IOS XEソフトウェアリリース16.9.1以降
- Cisco IOSソフトウェアリリース15.6(3)M7以降。15.7(3)M5以降または15.8(3)M3以降

ソフトウェアをアップグレードした後、自己署名証明書を再生成し、トラストストアで証明書を必要とするすべてのデバイスにエクスポートする必要があります。

ソフトウェアの即時アップグレードが不可能な場合は、次の3つの回避策があります。

1. 第3部認証局(CA)から有効な証明書を取得します。
2. Cisco IOS CAサーバを使用して、新しい証明書を生成します。
3. OpenSSLを使用して、新しい自己署名証明書を生成します。

1.サードパーティ認証局(CA)から有効な証明書を取得する

認証局から証明書をインストールします。一般的なCAには次のものがあります。 コモド、Let's 暗号化、RapidSSL、Thawte、Sectigo、GeoTrust、Symantecなど。この回避策を使用すると、証明書要求が生成され、Cisco IOSによって表示されます。その後、管理者は要求をコピーしてサードパーティCAに送信し、結果を取得します。

> **注：**CAを使用して証明書に署名することは、セキュリティのベストプラクティスと見なされます。この手順は、このField Noticeの回避策として提供されています。ただし、自己署

名証明書を使用するよりも、この回避策を適用した後もサードパーティのCA署名付き証明書を使用することを推奨します。

サードパーティCAから証明書をインストールするには、次の手順を実行します。

1. 証明書署名要求(CSR)を作成します。

```
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. CSRをサードパーティCAに送信します。**注：**CSRをサードパーティCAに送信し、証明書を取得する手順は、使用するCAによって異なります。この手順の実行方法については、CAのドキュメントを参照してください。
2. CA証明書とともに、ルータの新しいID証明書をダウンロードします。
3. デバイスにCA証明書をインストールします。

```
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. デバイスにID証明書をインストールします。

```
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. Cisco IOS CAサーバを使用した新しい証明書の生成

ローカルのCisco IOS Certificate Authorityサーバを使用して、新しい証明書を生成し、署名します。

注：ローカルCAサーバ機能は、一部の製品では使用できません。

```
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を使用した新しい自己署名証明書の生成

OpenSSLを使用してPKCS12証明書バンドルを生成し、バンドルをCisco IOSにインポートします。

LINUX、UNIX、またはMAC(OSX)の例

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またはCisco IOS XEルータの例

```
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
```

新しい証明書がインストールされていることを確認します。

```
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
```

> **注**：自己署名証明書は、2020年1月1日00:00 UTCに期限切れになり、それ以降は作成できません。

Q&A

Q：どこに問題があるか？

該当するCisco IOSまたはCisco IOS XEバージョンを実行する製品で生成された自己署名X.509

PKI証明書は、2020年1月1日00:00:00 UTCに期限切れになります。2020/01/01 00:00:00 UTC以降は、該当するデバイスに新しい自己署名証明書を作成できません。これらの自己署名証明書に依存するサービスは、証明書の有効期限が切れると機能しなくなります。

Q：製品の自己署名証明書が期限切れになると、クライアントネットワークにどのような影響がありますか。

自己署名証明書に依存する影響を受ける製品の機能は、証明書の有効期限が切れると機能しなくなります。詳細については、Field Noticeを参照してください。

Q：この問題の影響を受けているかどうかは、どうすればわかりますか。

Field Noticeでは、自己署名証明書を使用しているかどうか、および設定がこの問題に該当するかどうかを確認する手順を説明しています。Field Noticeの「該当製品の識別方法」セクションを参照してください。

Q：影響があるかどうかを確認するために実行できるスクリプトはありますか。

はい。Cisco CLIアナライザを使用して、System Diagnostic runを実行します。証明書が存在し、それが使用されている場合は、アラートを表示できます。https://cway.cisco.com/cli/

Q.この問題に対するソフトウェア修正はシスコから提供されていますか。

はい。シスコでは、この問題に対するソフトウェア修正をリリースしており、ソフトウェアのアップグレードがすぐに可能でない場合の回避策も提供しています。詳細については、Field Noticeを参照してください。

Q：この問題は、証明書を使用するシスコ製品に影響しますか。

いいえ。この問題**は、特定のバージョンのCisco IOSまたはCisco IOS XEによって生成され、製品のサービスに適用される証明書を持つ自己署名証明書を使用する製品にのみ影響を与えます。**認証局(CA)によって生成された証明書を使用する製品は、この問題の影響を受けません。

Q：シスコ製品は自己署名証明書のみを使用しますか。

いいえ。証明書は、外部のサードパーティ認証局(CA)、またはCisco IOSまたはCisco IOS XEデバイス自体で自己署名証明書として生成できます。特定のユーザ要件では、自己署名証明書の使用が必要になる場合があります。認証局(CA)によって生成された証明書は、この問題の影響を受けません。

Q.なぜこの問題が発生したのですか。

残念ながら、テクノロジーベンダーの最善の努力にもかかわらず、ソフトウェア不具合はまだ発生しています。シスコのテクノロジーにバグが発見された場合、シスコは透明性を確保し、ネットワークを保護するために必要な情報をユーザに提供することに尽力しています。

この場合、この問題は既知のソフトウェアの不具合が原因で発生しており、該当するCisco IOSおよびCisco IOS XEのバージョンでは、自己署名証明書の有効期限を常に2020年1月1日の00:00:00 UTCに設定できます。この日付以降は、証明書が期限切れになり無効になるため、製品の機能に

影響する可能性があります。

Q：有効期限として2020年1月1日00:00:00 UTCを選択したのはなぜですか。

証明書には通常、有効期限があります。このソフトウェアの不具合の場合、2020年1月1日の日付は10年以上前のCisco IOSおよびCisco IOS XEソフトウェアの開発期間中に使用されており、人為的なエラーです。

Q：この問題の影響を受ける製品は何ですか。

15.6(03)M07、15.7(03)M05、15.8(03)M03、および15.9(03)Mより前のCisco IOSリリースを実行するシスコ製品、および16.9.1より前のCisco IOS XEリリースを実行するシスコ製品

Q：ユーザは何をする必要がありますか。

Field Noticeを確認して、この問題による影響があるかどうかを評価し、影響がある場合は、回避策とソリューションの説明に従ってこの問題を軽減する必要があります。

Q：この問題はセキュリティの脆弱性ですか。

いいえ。これはセキュリティの脆弱性ではなく、製品の完全性に対するリスクもありません。

Q：SSHは影響を受けますか。

いいえ。SSHはRSAキーペアを使用しますが、まれな構成を除き、証明書を使用しません。
Cisco IOSで証明書を利用するには、次の設定が存在する必要があります。

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

Q：Classic Catalyst 2000、3000、4000、6000プラットフォームで使用できる修正バージョンは何ですか。

Polarisベースのプラットフォーム（3650/3850/Catalyst 9Kシリーズ）では、16.9.1以降で修正が利用可能
CDBプラットフォームでは、15.2(7)E1a以降で修正が利用可能です

その他のクラシックスイッチングプラットフォームの場合：

コミットは進行中ですが、CCOリリースは公開されていません。次のCCOリリースで修正できます。

インターンでは、他の利用可能な回避策のいずれかを利用してください。

Q：WAASは影響を受けますか。

WAASは引き続き正常に動作し、トラフィックを最適化しますが、AppNav-XEとCentral Managerは、期限切れの自己署名証明書を持つデバイスにオフラインになりました。つまり、AppNav-Clusterを監視したり、WAASのポリシーを変更したりすることはできません。要約する

と、WAASは引き続き正常に動作しますが、証明書の問題が解決されるまで、管理とモニタリングは中断されます。　この問題を解決するには、Cisco IOSで新しい証明書を生成し、Central Managerにインポートする必要があります。

関連情報

- FN70489 Field Notice:FN70489:Cisco IOSおよびCisco IOS XEソフトウェアでのPKI自己署名証明書の期限切れ
- Cisco Bug ID CSCvi48253

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。