IOS自簽名證書於2020年1月1日到期

目錄

簡介

本檔案介紹自簽證書(SSC)到期對思科軟體系統造成的影響及錯誤，並提供各種解決方法。

必要條件

需求

思科建議您瞭解以下主題：

- 自簽名證書(SSC)
- Cisco IOS®版本12.x及更高版本

採用元件

元件是受SSC到期影響的軟體系統。

所有使用自簽名證書、沒有Cisco錯誤ID CSCvi48253 修復或生成SSC時沒有Cisco錯誤ID CSCvi48253 修復的Cisco IOS和Cisco IOS® XE系統。其中包括：

- 所有Cisco IOS 12.x
- 15.6(3)M7、15.7(3)M5、15.8(3)M3、15.9(3)M3之前的所有Cisco IOS 15.x
- 16.9.1之前的所有Cisco IOS XE

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景

> **附註**：本文檔包含FN40789 的內容，以及其他上下文、示例、更新和問答。

2020 UTC 1月1日00:00，除非系統在生成SSC時運行固定版本的Cisco IOS和Cisco IOS XE，否則Cisco IOS和Cisco IOS XE系統上生成的所有自簽名證書(SSC)都將過期。此後，未修復的Cisco IOS系統無法生成新的SSC。任何依賴這些自簽名證書來建立或終止安全連線的服務在證書過期後都無法工作。

此問題僅影響由Cisco IOS或Cisco IOS XE裝置生成並應用於裝置上服務的自簽名證書。憑證授權單位(CA)產生的憑證（包括Cisco IOS CA功能產生的憑證）不會受到此問題的影響。

Cisco IOS和Cisco IOS XE軟體中的某些功能依賴數位簽章的X.509證書進行加密身份驗證。這些憑證是由外部第三方CA產生，或在Cisco IOS或Cisco IOS XE裝置上以自簽憑證方式產生。受影響的Cisco IOS和Cisco IOS XE軟體版本將自簽名證書到期日期設定為2020-01-01 00:00:00 UTC。在此日期之後，證書將過期且無效。

可依賴自簽名證書的服務包括：

一般功能

- HTTP Server over TLS(HTTPS)- HTTPS在瀏覽器中生成錯誤，指示證書已過期。
- SSH伺服器 — 使用X.509證書對SSH會話進行身份驗證的使用者可能無法進行身份驗證。(很少使用X.509憑證。使用者名稱/密碼身份驗證和公鑰/私鑰身份驗證不受影響。)
- RESTCONF - RESTCONF連線可能失敗。

合作功能

- 使用TLS的作業階段啟始通訊協定(SIP)
- 已啟用加密訊號的Cisco Unified Communications Manager Express(CME)

- 已啟用加密訊號的Cisco整合Survivable遠端站點電話(SRST)
- Cisco IOS dspfarm 已啟用加密信令的資源（會議、媒體終端點或轉碼）
- 精簡型使用者端控制通訊協定(SCCP)電話控制應用程式(STCAPP)連線埠設定為加密訊號
- 媒體閘道控制通訊協定(MGCP)和H.323使用IP安全的通話訊號(IPSec)（不含預先共用金鑰）
- 安全模式下的Cisco Unified Communications Gateway Services API（使用HTTPS）

無線功能

- 舊版Cisco IOS接入點（在2005年或更早版本生產）與無線LAN控制器之間的LWAPP/CAPWAP連線。如需詳細資訊，請參閱Cisco Field Notice FN63942。

問題

嘗試在受影響的Cisco IOS或Cisco IOS XE軟體版本2020-01-01 00:00:00 UTC之後生成自簽名證書會導致以下錯誤：

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

任何依賴自簽名證書的服務均無法正常工作。例如：

- SIP over TLS呼叫未完成。
- 註冊到Cisco Unified CME且已啟用加密信令的裝置不再起作用。
- 已啟用加密信令的Cisco Unified SRST不允許裝置註冊。
- 已啟用加密訊號的Cisco IOS dspfarm資源（會議、媒體終端點或轉碼）將不再註冊。
- 使用加密信令配置的STCAPP埠不再註冊。
- 通過網關進行的呼叫可能會失敗，如果沒有預共用金鑰，則MGCP或H.323會通過IPSec呼叫信令。
- 在安全模式下使用Cisco Unified Communications Gateway Services API（使用HTTPS）的API呼叫可能會失敗。
- RESTCONF可能失敗。
- 用於管理裝置的HTTPS會話顯示瀏覽器警告，指示證書已過期。
- AnyConnect SSL VPN會話無法建立或報告無效證書。
- IPSec連線可能無法建立。

如何識別受影響的產品

> **附註**：要受到此現場通知的影響，裝置*必須定義自簽名證書，且自簽名證書必須應用於下面概述的一個或多個功能*。當證書到期時，單獨存在自簽名證書不會影響裝置的運行，無需立即執行操作。**裝置必須符合以下第3步和第4步中的標準，才會受到影響。**

確定是否使用自簽名證書：

1. 輸入 show running-config | begin crypto 命令。
2. 查詢加密PKI信任點配置。
3. 在加密PKI信任點配置中，查詢信任點註冊配置。信任點註冊必須配置為影響**「自簽」**。此外，自簽名證書也必須出現在配置中。請注意，信任點名稱不包含如下例所示的「self-signed」字樣。

```
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
```

如果未將信任點註冊*配置為*「selfsigned」；則裝置不受此欄位通知的影響。不需要執行任何操作。如果信任點註冊*配置為「自簽名」*，**且配置中顯示自簽名證書**；則裝置可能受到此欄位通知的影響。繼續步驟4。

4. 如果您在步驟3中確定信任點註冊配置為「自簽名」，並且自簽名證書顯示在配置中，則檢查自簽名證書是否應用於裝置上的功能。以下示例配置顯示了可以與SSC關聯的各種功能：

- 對於**HTTPS伺服器**，必須存在以下文本：

```
ip http secure-server
```

此外，還可以定義信任點，如下面的代碼示例所示。如果此命令不存在，則預設行為是使用自簽名證書。

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

如果定義了信任點，且它指向自簽名證書以外的證書，則不會影響您。

對於**HTTPS伺服器**，證書過期的影響較小，因為自簽名證書已被Web瀏覽器解除信任，即使未過期，也會生成警告。如果證書過期，可能會更改在瀏覽器中收到的警告。

- 對於**SIP over TLS**，此文本顯示在配置檔案中：

```
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>
!
```

- 對於啟用了加密信令的**Cisco Unified CME**，此文本顯示在配置檔案中：

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

- 對於啟用了加密信令的**Cisco Unified SRST**，此文本顯示在配置檔案中：

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

- 對於 **Cisco IOS dspfarm 資源**在已啟用加密訊號的情況下（會議、媒體終端點或轉碼），組態檔中會顯示以下文字：

```
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>
!
```

- 對於**使用加**密訊號設定的STCAPP連線埠，組態檔中會顯示以下文字：

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

- 對於在安全模式下的**Cisco Unified Communications Gateway Services API**，此文本顯示在配置檔案中：

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

- 對於**SSLVPN**，此文本顯示在配置檔案中：

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

OR

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

- 對於**ISAKMP和IKEv2**，如果存在任何配置，則可以使用自簽名證書（需要對配置進行進一步分析，以確定功能是否使用自簽名證書而不是使用其他證書）：

```
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
```

- 對於**SSH伺服器**，極不可能利用證書對SSH會話進行身份驗證。但是您可以檢查您的組態來驗證這點。您必須將所有三行都顯示在下一個代碼示例中，才能受到影響。 **附註**：如果您使用使用者名稱和密碼組合通過SSH連線到裝置，則不會受到影響。

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

- 若是**RESTCONF**，組態檔中會顯示以下文字：

```
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
```

解決方案

解決方案是將Cisco IOS或Cisco IOS XE軟體升級到包含修復程式的版本：

- Cisco IOS XE軟體版本16.9.1及更高版本
- Cisco IOS軟體版本15.6(3)M7及更新版本；15.7(3)M5及更高版本；或15.8(3)M3及更高版本

升級軟體後，必須重新生成自簽名證書，並將其匯出到可能在其信任儲存中需要該證書的任何裝置

。

如果無法立即進行軟體升級，有三種變通方案可用：

1. 從第三方憑證授權單位(CA)取得有效憑證。
2. 使用Cisco IOS CA伺服器生成新證書。
3. 使用OpenSSL產生新的自簽名證書。

1.從第三方證書頒發機構(CA)獲取有效證書

從證書頒發機構安裝證書。常見CA包括： 科莫多， Let's Encrypt、RapidSSL、Thawte、Sectigo、GeoTrust、Symantec等。通過此解決方法，Cisco IOS會生成並顯示證書請求。然後，管理員複製請求，將其提交給第三方CA，並檢索結果。

> **附註**：使用CA簽署憑證視為資安最佳常規。本程式作為本現場通知的變通方法提供；但是，在應用此解決方法後，最好繼續使用第三方CA簽名的證書，而不是使用自簽名證書。

從第三方CA安裝證書：

1. 建立憑證簽署請求(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. 將CSR提交給第三方CA。**附註**：將CSR提交給第三方CA和擷取結果的程式會因使用的CA而異。有關如何執行此步驟的說明，請參閱CA的文檔。
2. 下載路由器的新身分憑證以及CA憑證。
3. 在裝置上安裝CA證書：

```
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. 在裝置上安裝身份證書：

```
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.使用Cisco IOS CA伺服器生成新證書

使用本地Cisco IOS證書頒發機構伺服器生成新證書並對其簽名。

注意：本地CA伺服器功能並非在所有產品上都可用。

```
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.使用OpenSSL生成新的自簽名證書

使用OpenSSL產生PKCS12憑證套件組合，並將套件組合匯入Cisco IOS。

LINUX、UNIX或MAC(OSX)示例

```
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或Cisco IOS XE路由器示例

```
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
```

驗證是否已安裝新憑證：

```
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
```

附註：自簽名證書在2020年1月1日00:00過期，並且在該時間之後無法建立。

問答

Q:問題是什麼？

在運行受影響的Cisco IOS或Cisco IOS XE版本的產品上生成的自簽名X.509 PKI證書在01/01/2020 00:00:00 UTC到期。在01/01/2020 00:00:00 UTC之後，無法在受影響的裝置上建立新的自簽名證書。任何依賴這些自簽名證書的服務在證書過期後都無法再工作。

Q:如果自簽名證書對其產品過期，會對客戶端網路產生什麼影響？

任何依賴自簽名證書的受影響產品的功能在證書過期後都無法再工作。有關其他詳細資訊，請參閱現場通知。

Q:如何知道我是否受此問題影響？

該現場通知提供相關說明，用於確定您是否使用自簽名證書以及您的配置是否受此問題影響。請參閱現場通知中的「如何識別受影響的產品」部分。

Q:是否有指令碼可以運行以檢視我是否受到影響？

會。使用Cisco CLI Analyzer運行系統診斷程式。如果存在證書並且已使用該證書，則可以顯示警報。https://cway.cisco.com/cli/

問：思科是否針對此問題提供了軟體修復？

會。思科已針對此問題發佈了軟體修復程式，以及在軟體升級無法立即實現時採取的解決方法。有關完整詳情，請參閱「現場通知」。

Q:此問題是否會影響任何使用憑證的思科產品？

否。此問題僅影響使用由特定版本的**Cisco IOS或Cisco IOS XE生成的自簽名證書以及應用於產品上服務的證書的產**品。使用憑證授權單位(CA)產生的憑證的產品不受此問題影響。

Q:思科產品是否僅使用自簽名證書？

不能。憑證可由外部第三方憑證授權單位產生，或在Cisco IOS或Cisco IOS XE裝置上以自簽憑證方式產生。特定使用者要求可能要求使用自簽名證書。證書頒發機構(CA)生成的證書不受此問題的影響。

問：為什麼會出現此問題？

遺憾的是，儘管技術供應商盡了最大努力，軟體缺陷仍會出現。當在任何思科技術中發現錯誤時，我們承諾保持透明，並向我們的使用者提供保護網路所需的資訊。

在這種情況下，問題是由已知軟體錯誤引起的，在該軟體錯誤中，受影響的Cisco IOS和Cisco IOS XE版本始終可以將自簽名證書的過期日期設定為01/01/2020 00:00:00 UTC。在此日期之後，證書將過期且無效，這可能會影響產品功能。

Q:為什麼選擇2020年1月1日00:00:00 UTC的到期日期？

證書通常具有到期日期。對於此軟體錯誤，2020年1月1日是10多年前在Cisco IOS和Cisco IOS XE軟體開發期間使用的日期，這是一個人為錯誤。

Q:哪些產品受此問題影響？

運行15.6(03)M07、15.7(03)M05、15.8(03)M03和15.9(03)M之前的Cisco IOS版本的任何思科產品，以及運行16.9.1之前的Cisco IOS XE版本的任何思科產品

Q:使用者需要做什麼？

您需要檢視現場通知，以評估您是否受到此問題的影響，如果是，則按照解決方法/解決方案說明來緩解此問題。

Q:此問題是安全漏洞嗎？

不。這不是安全漏洞，並且不存在對產品完整性的風險。

Q:SSH是否受影響？

不能。 SSH使用RSA金鑰對，但不會使用證書（在極少數配置中除外）。要使Cisco IOS使用證書，必須存在下一個配置。

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

Q:傳統Catalyst 2K、3K、4K和6K平台提供哪些固定版本？

對於基於Polaris的平台（3650/3850/Catalyst 9K系列），16.9.1以後可用fix
對於CDB平台，從15.2(7)E1a開始提供修復

對於其他傳統交換平台：

提交正在進行，但我們尚未發佈CCO版本。下一個CCO版本可以有修復。

在過渡期內，請利用其他可用的變通方法之一。

Q:WAAS受影響嗎？

WAAS繼續正常運行並最佳化流量，但是，AppNav-XE和中央管理器離線訪問具有過期自簽名證書的裝置。這意味著您無法監視AppNav群集或更改WAAS的任何策略。總而言之，WAAS可繼續正常工作，但管理和監控會暫停，直到證書問題得到解決。 要解決此問題，可能需要在Cisco IOS上生成新證書，然後將其匯入到中央管理器中。

相關資訊

- 請參閱FN70489現場通知：FN - 70489 - Cisco IOS和Cisco IOS XE軟體中的PKI自簽名證書過期
- 請參閱思科錯誤ID CSCvi48253

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。