IOS自签名证书将于2020年1月1日到期

目录

简介

本文档介绍自签名证书(SSC)在思科软件系统中到期时造成的影响和错误，并提供各种解决方法。

先决条件

要求

Cisco 建议您了解以下主题：

- 自签名证书(SSC)
- Cisco IOS® 12.x版及更高版本

使用的组件

组件是受SSC到期影响的软件系统。

所有Cisco IOS和Cisco IOS® XE系统使用自签名证书，没有Cisco Bug ID CSCvi48253修复，或者生成SSC时没有Cisco Bug ID CSCvi48253修复。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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景

> **注意**：本文档包含FN40789的内容，以及其他上下文、示例、更新和问答。

在2020年1月1日00:00 UTC，除非系统在生成SSC时运行固定版本的Cisco IOS和Cisco IOS XE，否则在Cisco IOS和Cisco IOS XE系统上生成的所有自签名证书(SSC)均设置为过期。此后，未修复的Cisco IOS系统无法生成新的SSC。依靠这些自签名证书建立或终止安全连接的任何服务在证书过期后都不会工作。

此问题仅影响由Cisco IOS或Cisco IOS XE设备生成并应用于设备上服务的自签名证书。证书颁发机构(CA)生成的证书（包括Cisco IOS CA功能生成的证书）不受此问题的影响。

Cisco IOS和Cisco IOS XE软件中的某些功能依赖于数字签名的X.509证书进行加密身份验证。这些证书由外部第三方CA生成，或在Cisco IOS或Cisco IOS XE设备上生成自签名证书。受影响的Cisco IOS和Cisco IOS XE软件版本将自签名证书到期日期设置为2020-01-01 00:00:00 UTC。在此日期之后，证书将过期且无效。

可依赖自签名证书的服务包括：

一般功能

- HTTP Server over TLS(HTTPS)- HTTPS在浏览器中生成错误，指示证书已过期。
- SSH服务器 — 使用X.509证书对SSH会话进行身份验证的用户可能无法进行身份验证。(很少使用X.509证书。用户名/密码身份验证和公钥/私钥身份验证不受影响。)
- RESTCONF - RESTCONF连接可能失败。

协作功能

- TLS上的会话发起协议(SIP)
- 启用加密信令的Cisco Unified Communications Manager Express(CME)

- 启用加密信令的Cisco Unified Survivable Remote Site Telephony(SRST)
- Cisco IOS dspfarm 启用加密信令的资源（会议、媒体终端点或转码）
- 配置了加密信令的瘦客户端控制协议(SCCP)电话控制应用(STCAPP)端口
- 媒体网关控制协议(MGCP)和H.323 IP安全呼叫信令(IPSec)，无预共享密钥
- 安全模式下的思科统一通信网关服务API（使用HTTPS）

无线功能

- 旧式Cisco IOS接入点（在2005年或更早版本生产）和无线LAN控制器之间的LWAPP/CAPWAP连接。有关详细信息，请参阅Cisco Field Notice FN63942。

问题

尝试在受影响的Cisco IOS或Cisco IOS XE软件版本2020-01-01 00:00:00 UTC之后生成自签名证书会导致以下错误：

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

依赖自签名证书的任何服务均不起作用。例如：

- SIP over TLS呼叫未完成。
- 注册到Cisco Unified CME且启用了加密信令的设备不再起作用。
- 启用加密信令的Cisco Unified SRST不允许设备注册。
- 启用加密信令的Cisco IOS dspfarm资源（会议、媒体终端点或转码）不再注册。
- 配置了加密信令的STCAPP端口不再注册。
- 通过网关进行的呼叫可能会失败，MGCP或H.323会通过IPSec呼叫信令，而无需预共享密钥。
- 在安全模式下使用思科统一通信网关服务API（使用HTTPS）的API调用可能会失败。
- RESTCONF可能会失败。
- 用于管理设备的HTTPS会话显示浏览器警告，指示证书已过期。
- AnyConnect SSL VPN会话无法建立或报告无效证书。
- IPSec连接可能无法建立。

如何确定受影响的产品

> **注意：**要受到此现场通知的影响，设备*必须*定义自签名证书，*且自签名证书必须应用于下述一个或多个功能*。当证书到期时，仅存在自签名证书不会影响设备的运行，不需要立即采取措施。**设备必须满足以下第3步和第4步中的条件才能受到影响。**

要确定是否使用自签名证书，请执行以下操作：

1. 输入 show running-config | begin crypto 命令。
2. 查找crypto PKI trust-point配置。
3. 在加密PKI信任点配置中，查找信任点注册配置。信任点注册必须配置为影响**“自签**”。此外，自签名证书也必须出现在配置中。请注意，信任点名称不包含如下例所示的“self-signed”字样。

```
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
```

如果未将信任点注册*配置为*"自签名"；设备不受此现场通知的影响。不需要采取任何操作。如果信任点注册*配置为"自签名"*，并且配置中显示自签名证书；设备可能受到此字段通知的影响。继续执行第 4 步。

4. 如果在步骤3中确定信任点注册配置为"自签名"，并且自签名证书显示在配置中，则检查自签名证书是否应用于设备上的功能。以下示例配置显示了可与SSC关联的各种功能：

- 对于**HTTPS服务器**，必须存在以下文本：

```
ip http secure-server
```

此外，信任点也可以定义如下一个代码示例所示。如果此命令不存在，则默认行为是使用自签名证书。

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

如果定义了信任点，且它指向自签名证书以外的证书，则不会受到影响。

对于**HTTPS服务器**，过期证书的影响较小，因为自签名证书已被Web浏览器解除信任并生成警告（即使未过期）。过期证书的存在会更改在浏览器中收到的警告。

- 对于**SIP over TLS**，此文本出现在配置文件中：

```
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>
!
```

- 对于启用了加密信令的**Cisco Unified CME**，此文本出现在配置文件中：

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

- 对于启用了加密信令的**Cisco Unified SRST**，此文本出现在配置文件中：

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

- 对于 **Cisco IOS dspfarm 资源**在启用加密信令的情况下（会议、媒体终端点或转码），以下文本出现在配置文件中：

```
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>
!
```

- 对于**使用加密**信令配置的STCAPP端口，此文本出现在配置文件中：

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

- 对于**安全模式下的思科统一通信网关服务API**，此文本出现在配置文件中：

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

- 对于**SSLVPN**，此文本出现在配置文件中：

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

OR

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

- 对于**ISAKMP和IKEv2**，如果存在任何配置，可以使用自签名证书（需要对配置进行进一步分析，以确定功能是否使用自签名证书而不是其他证书）：

```
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
```

- 对于**SSH服务器**，极不可能利用证书对SSH会话进行身份验证。但是，您可以检查配置以验证这一点。您必须有所有三行在下一个代码示例中显示，才会受到影响。 **注意：**如果使用用户名和密码组合通过SSH连接到设备，则不会受到影响。

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

- 对于**RESTCONF**，此文本出现在配置文件中：

```
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
```

解决方案

解决方案是将Cisco IOS或Cisco IOS XE软件升级到包含修复程序的版本：

- Cisco IOS XE软件版本16.9.1及更高版本
- Cisco IOS软件版本15.6(3)M7及更高版本；15.7(3)M5及更高版本；或15.8(3)M3及更高版本

升级软件后，必须重新生成自签名证书，并将其导出到可以在其信任存储中需要该证书的任何设备。

如果无法立即进行软件升级，有三种变通方案可用：

1. 从第三方证书颁发机构(CA)获取有效证书。
2. 使用Cisco IOS CA服务器生成新证书。
3. 使用OpenSSL生成新的自签名证书。

1.从第三方证书颁发机构(CA)获取有效证书

从证书颁发机构安装证书。常见CA包括： 科莫多， Let's Encrypt、RapidSSL、Thawte、Sectigo、GeoTrust、Symantec等。通过此解决方法，Cisco IOS会生成并显示证书请求。然后，管理员复制请求，将其提交给第三方CA，并检索结果。

> **注意：**使用CA签署证书被视为一种安全最佳实践。此步骤在此现场通知中作为解决方法提供；但是，在应用此解决方法后，最好继续使用第三方CA签名的证书，而不是使用自签证书。

要安装来自第三方CA的证书，请执行以下操作：

1. 创建证书签名请求(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. 向第三方CA提交CSR。**注意：**向第三方CA提交CSR并检索结果的证书的过程因使用的CA而异。有关如何执行此步骤的说明，请参阅您的CA的文档。
2. 下载路由器的新身份证书以及CA证书。
3. 在设备上安装CA证书：

```
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. 在设备上安装身份证书：

```
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服务器生成新证书

使用本地Cisco IOS Certificate Authority服务器生成并签署新证书。

注意：本地CA服务器功能并非在所有产品上都可用。

```
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生成新的自签名证书

使用OpenSSL生成PKCS12证书捆绑包并将捆绑包导入到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
```

验证新证书是否已安装：

```
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
```

注意：自签名证书在2020年1月1日00:00到期，之后无法创建。

问题解答

问：问题是什么？

运行受影响的Cisco IOS或Cisco IOS XE版本的产品生成的自签名X.509 PKI证书在01/01/2020 00:00:00 UTC到期。在01/01/2020 00:00:00 UTC之后，无法在受影响的设备上创建新的自签名证书。在证书过期后，依赖于这些自签名证书的任何服务都无法再工作。

问：如果自签名证书对其产品到期，会对客户端网络造成什么影响？

依赖于自签名证书的任何受影响产品的功能在证书过期后将无法继续工作。有关其他详细信息，请参阅“现场通知”。

问：如何知道自己是否受到此问题的影响？

现场通知提供相关说明，以确定您是否使用自签名证书以及您的配置是否受到此问题的影响。请参阅现场通知中的“如何识别受影响的产品”部分。

问：是否有脚本可以运行以查看我是否受到影响？

Yes.使用Cisco CLI分析器运行系统诊断运行。如果存在证书并且已使用该证书，则可以显示警报。https://cway.cisco.com/cli/

问：思科是否针对此问题提供了软件修复程序？

Yes.思科已针对此问题发布了软件修复程序，并在软件升级不可立即实施的情况下发布了解决方法。有关完整详情，请参阅“现场通知”。

问：此问题是否影响任何使用证书的思科产品？

否。此问题仅影响使用由特定版本的**Cisco IOS或Cisco IOS XE生成的自签名证书以及应用于产品上的服务的证书的产**品。使用证书颁发机构(CA)生成的证书的产品不受此问题的影响。

问：思科产品是否仅使用自签名证书？

不能。证书可由外部第三方证书颁发机构生成，也可以在Cisco IOS或Cisco IOS XE设备上生成自签名证书。特定用户要求可能要求使用自签名证书。证书颁发机构(CA)生成的证书不受此问题的影响。

问：为什么会出现此问题？

遗憾的是，尽管技术供应商尽了最大努力，软件缺陷仍然会出现。当在任何思科技术中发现漏洞时，我们致力于保持透明度，并向用户提供保护网络所需的信息。

在本例中，问题由已知软件Bug引起，在该软件中，受影响的Cisco IOS和Cisco IOS XE版本始终可以将自签名证书的到期日期设置为01/01/2020 00:00:00 UTC。在此日期之后，证书将过期且无效，这可能会影响产品功能。

问：为什么选择2020年1月1日00:00:00 UTC的到期日期？

证书通常具有到期日期。对于此软件Bug，2020年1月1日是十多年前在Cisco IOS和Cisco IOS XE软件开发期间使用的，这是一个人为错误。

问：哪些产品受此问题影响？

运行早于15.6(03)M07、15.7(03)M05、15.8(03)M03和15.9(03)M的Cisco IOS版本的任何思科产品，以及运行早于16.9.1的Cisco IOS XE版本的任何思科产品

问：用户需要做什么？

您需要查看现场通知，以评估您是否已受到此问题的影响，如果是，请按照解决方法/解决方案的说明来缓解此问题。

问：此问题是安全漏洞吗？

不会。这不是一个安全漏洞，且不存在影响产品完整性的风险。

问：SSH是否受影响？

否。 SSH使用RSA密钥对，但不会使用证书，除非在极少数配置中。要使Cisco IOS使用证书，必须存在下一个配置。

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

问：传统Catalyst 2K、3K、4K、6K平台有哪些固定版本？

对于基于Polaris的平台（3650/3850/Catalyst 9K系列），可从16.9.1以后进行修复
对于CDB平台，从15.2(7)E1a开始提供修复

对于其他传统交换平台：

提交正在进行，但我们尚未发布CCO版本。下一个CCO版本可以修复。

请在中间位置使用其他可用的变通方法。

问：WAAS受影响吗？

WAAS可继续正常运行并优化流量，但是，AppNav-XE和中央管理器已离线到具有过期自签名证书的设备。这意味着您无法监控AppNav群集或更改WAAS的任何策略。总之，WAAS可继续正常工作，但管理和监控会暂停，直到证书问题解决为止。 要解决此问题，可能需要在Cisco IOS上生成新证书，然后导入到中央管理器。

相关信息

- 请参阅FN70489现场通知：FN - 70489 - Cisco IOS和Cisco IOS XE软件中的PKI自签名证书过

期

- 请参阅Cisco Bug ID CSCvi48253

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。