Vencimiento del certificado autofirmado de IOS el 1 de enero de 2020

Contenido

Introducción

Este documento describe los efectos y errores causados por el vencimiento de los certificados autofirmados (SSC) en los sistemas de software de Cisco y proporciona varias soluciones alternativas.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Certificados con firma automática (SSC)
- Cisco IOS® versión 12.x y posteriores

Componentes Utilizados

Los componentes son los sistemas de software afectados por el vencimiento del SSC.

Todos los sistemas Cisco IOS y Cisco IOS® XE que utilizan un certificado autofirmado, que no tienen el ID de bug de Cisco CSCvi48253 corregido, o que no tenían el ID de bug de Cisco CSCvi48253 cuando se generó el SSC. Esto incluye:

- Todo el IOS 12.x de Cisco
- Todos los Cisco IOS 15.x anteriores a 15.6(3)M7, 15.7(3)M5, 15.8(3)M3, 15.9(3)M
- Todos los Cisco IOS XE anteriores a 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Background

> **Nota:** Este documento contiene el contenido de FN40789 , junto con contexto adicional, ejemplos, actualizaciones y preguntas y respuestas.

A las 00:00 del 1 de enero de 2020 UTC, todos los certificados autofirmados (SSC) generados en los sistemas Cisco IOS y Cisco IOS XE estaban configurados para caducar, a menos que el sistema ejecutara una versión fija de Cisco IOS y Cisco IOS XE cuando se generó el SSC. Después de ese tiempo, los sistemas Cisco IOS no fijos no pueden generar nuevos SSC. Cualquier servicio que se base en estos certificados autofirmados para establecer o finalizar una conexión segura no funciona después de que caduque el certificado.

Este problema afecta solamente a los certificados autofirmados que fueron generados por el dispositivo Cisco IOS o Cisco IOS XE y aplicados a un servicio en el dispositivo. Este problema no afecta a los certificados generados por una autoridad de certificación (CA), que incluye los certificados generados por la función CA de Cisco IOS.

Ciertas funciones del software Cisco IOS y Cisco IOS XE se basan en certificados X.509 firmados digitalmente para la validación de identidad criptográfica. Estos certificados los genera una CA externa de terceros o en el propio dispositivo Cisco IOS o Cisco IOS XE como certificado autofirmado. Las versiones afectadas del software Cisco IOS y Cisco IOS XE establecen la fecha de vencimiento del certificado de firma automática en 2020-01-01 00:00:00 UTC. Después de esta fecha, el certificado caduca y no es válido.

Los servicios que pueden depender de un certificado autofirmado incluyen:

Características generales

- HTTP Server over TLS (HTTPS): HTTPS produce un error en el navegador que indica que el certificado ha caducado.
- Servidor SSH: Los usuarios que utilizan certificados X.509 para autenticar la sesión SSH pueden no autenticarse. (El uso de certificados X.509 es poco frecuente. La autenticación de nombre de usuario/contraseña y la autenticación de clave pública/privada no se ven afectadas.)
- RESTCONF - Las conexiones RESTCONF pueden fallar.

Funciones de colaboración

- Protocolo de inicio de sesión (SIP) sobre TLS
- Cisco Unified Communications Manager Express (CME) con señalización cifrada habilitada
- Cisco Unified Survivable Remote Site Telephony (SRST) con señalización cifrada habilitada
- IOS de Cisco dspfarm recursos (conferencia, punto de terminación de medios o transcodificación) con la señalización cifrada habilitada
- Puertos de la aplicación de control de telefonía (STCAPP) del protocolo de control de clientes skinny (SCCP) configurados con señalización cifrada
- Protocolo de control de gateway de medios (MGCP) y señalización de llamadas H.323 sobre seguridad IP (IPSec) sin clave previamente compartida
- API de servicios de Cisco Unified Communications Gateway en modo seguro (que utiliza HTTPS)

Funciones inalámbricas

- Conexiones LWAPP/CAPWAP entre los puntos de acceso Cisco IOS anteriores (fabricados en 2005 o antes) y el controlador de LAN inalámbrica. Consulte Cisco Field Notice FN63942 para obtener más detalles.

Problema

Un intento de generar un certificado autofirmado en una versión de software afectada de Cisco IOS o Cisco IOS XE después de 2020-01-01 00:00:00 UTC produce este error:

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

Los servicios que dependen del certificado autofirmado no funcionan. Por ejemplo:

- Las llamadas SIP sobre TLS no se completan.
- Los dispositivos registrados en Cisco Unified CME con la señalización cifrada habilitada ya no funcionan.
- Cisco Unified SRST con señalización cifrada habilitada no permite el registro de dispositivos.
- Los recursos dspfarm de Cisco IOS (Conference, Media Termination Point o Transcoding) con la señalización cifrada habilitada ya no se registran.

- Los puertos STP configurados con señalización cifrada ya no se registran.
- Las llamadas a través de una gateway que realizan señalización de llamada MGCP o H.323 a través de IPSec sin una clave previamente compartida pueden fallar.
- Las llamadas a la API que utilizan la API de servicios de Cisco Unified Communications Gateway en modo seguro (que utilizan HTTPS) pueden fallar.
- RESTCONF puede fallar.
- Las sesiones HTTPS para administrar el dispositivo muestran una advertencia del navegador, que indica que el certificado ha caducado.
- Las sesiones VPN SSL de AnyConnect no pueden establecer o informar de un certificado no válido.
- Las conexiones IPSec no se pueden establecer.

Cómo identificar los productos afectados

> **Nota:** Para verse afectado por este aviso de campo, un dispositivo debe tener definido un certificado autofirmado *y* el certificado autofirmado debe aplicarse a una o más funciones como se describe a continuación. La presencia de un certificado autofirmado por sí solo no afecta al funcionamiento del dispositivo cuando caduca el certificado y no requiere ninguna acción inmediata. **Para que un dispositivo se vea afectado, debe cumplir los criterios de los pasos 3 y 4 siguientes.**

Para determinar si utiliza un certificado autofirmado:

1. Escriba el show running-config | begin crypto en el dispositivo.
2. Busque la configuración crypto PKI trust-point.
3. En la configuración crypto PKI trust-point, busque la configuración de inscripción de punto de confianza. La inscripción en el punto de confianza debe configurarse para que se vea afectada la **firma** automática. Además, el certificado autofirmado también debe aparecer en la configuración. Observe que el nombre del punto de confianza no contiene las palabras "autofirmado", como se muestra en el siguiente ejemplo.

```
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 la inscripción de punto de confianza *no* **está configurada para** "autofirmado"; **el dispositivo NO se ve afectado por este aviso de campo**. No se requiere ninguna acción.**Si la inscripción de punto de confianza** *se* **configura para "autofirmado" y si el certificado autofirmado aparece en la configuración**; el **dispositivo puede verse afectado** por este aviso de campo. Continúe con el paso 4.
4. Si en el paso 3 determinó que la inscripción de punto de confianza está configurada para "autofirmado" y que el certificado autofirmado aparece en la configuración, compruebe si el certificado autofirmado se aplica a una función del dispositivo.En estas configuraciones de ejemplo se muestran varias funciones que se pueden vincular al SSC:

- Para **HTTPS Server**, este texto debe estar presente:

```
ip http secure-server
```

Además, un punto de confianza también se puede definir como se muestra en el siguiente ejemplo de código. Si este comando no está presente, el comportamiento predeterminado es utilizar el Certificado autofirmado.

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

Si se define un punto de confianza y éste apunta a un certificado que no sea el Certificado autofirmado, no se verá afectado.

Para **HTTPS Server**, el impacto del certificado caducado es menor porque los certificados autofirmados ya no son fiables para los navegadores web y generan una advertencia incluso cuando no han caducado. La presencia de un certificado caducado puede cambiar la advertencia que recibe en el explorador.

- Para **SIP sobre TLS**, este texto está presente en el archivo de configuración:

```
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>
!
```

- Para **Cisco Unified CME** con la señalización cifrada habilitada, este texto está presente en el archivo de configuración:

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

- Para **Cisco Unified SRST** con la señalización cifrada habilitada, este texto está presente en el archivo de configuración:

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

- Para **IOS de Cisco dspfarm recursos** (Conferencia, Punto de terminación de medios o Transcodificación) con la señalización cifrada habilitada, este texto está presente en el archivo de configuración:

```
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>
```

```
!
```

- Para los **puertos STP** configurados con señalización cifrada, este texto está presente en el archivo de configuración:

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

- Para **Cisco Unified Communications Gateway Services API en modo seguro**, este texto está presente en el archivo de configuración:

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

- Para **SSLVPN**, este texto está presente en el archivo de configuración:

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

OR

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

- Para **ISAKMP e IKEv2**, se puede utilizar el certificado autofirmado si alguna de las configuraciones está presente (se requiere un análisis adicional de la configuración para determinar si la función utiliza el certificado autofirmado frente a un certificado diferente):

```
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
```

- Para **SSH Server**, es extremadamente improbable que pueda aprovechar los certificados para autenticar las sesiones SSH. Sin embargo, puede comprobar la configuración para comprobarlo. Debe tener las tres líneas mostradas en el siguiente ejemplo de código para que se vean afectadas. **Nota:** Si ha aprovechado la combinación de nombre de usuario y contraseña para SSH en su dispositivo, NO se verá afectado.

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

- Para **RESTCONF**, este texto está presente en el archivo de configuración:

```
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
```

Solución(es)

La solución consiste en actualizar el software Cisco IOS o Cisco IOS XE a una versión que incluya la corrección:

- Versión 16.9.1 y posteriores del software Cisco IOS XE
- Cisco IOS Software Release 15.6(3)M7 y posterior; 15.7(3)M5 y posteriores; o 15.8(3)M3 y posterior

Después de actualizar el software, debe volver a generar el certificado autofirmado y exportarlo a cualquier dispositivo que pueda requerir el certificado en su almacén de confianza.

Hay tres soluciones alternativas disponibles si no es posible realizar una actualización de software inmediata:

1. Obtenga un certificado válido de una autoridad de certificación (CA) de terceros.
2. Utilice el servidor de CA de Cisco IOS para generar un nuevo certificado.
3. Utilice OpenSSL para generar un nuevo certificado autofirmado.

1. Obtenga un certificado válido de una autoridad de certificación (CA) de terceros

Instale un certificado de una entidad emisora de certificados. Las CA comunes incluyen: Comodo, Let's Encrypt, RapidSSL, Thawte, Sectigo, GeoTrust, Symantec, etc. Con esta solución alternativa, Cisco IOS genera y muestra una solicitud de certificado. A continuación, el administrador copia la solicitud, la envía a una CA de terceros y recupera el resultado.

> **Nota:** El uso de una CA para firmar certificados se considera una práctica recomendada de seguridad. Este procedimiento se proporciona como solución alternativa en este aviso de campo; sin embargo, es preferible seguir utilizando el certificado firmado por CA de terceros después de aplicar esta solución alternativa, en lugar de utilizar un certificado firmado automáticamente.

Para instalar un certificado de una CA de terceros:

1. Crear una solicitud de firma de certificado (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. Envíe el CSR a la CA de terceros.**Nota:** El procedimiento para enviar el CSR a una CA de terceros y recuperar el certificado resultante varía en función de la CA que se utilice. Consulte la documentación de la CA para obtener instrucciones sobre cómo realizar este paso.
2. Descargue el nuevo certificado de identidad para el router junto con el certificado de CA.
3. Instale el certificado de la CA en el dispositivo:

```
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. Instale el certificado de identidad en el dispositivo:

```
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. Utilice el servidor de CA de Cisco IOS para generar un nuevo certificado

Utilice el servidor local de la autoridad certificadora de Cisco IOS para generar y firmar un nuevo certificado.

Nota: la función de servidor de la CA local no está disponible en todos los productos.

```
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. Utilice OpenSSL para generar un nuevo certificado autofirmado

Utilice OpenSSL para generar un paquete de certificados PKCS12 e importar el paquete a Cisco IOS.

Ejemplo de LINUX, UNIX o 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
```

Ejemplo de Router Cisco IOS o 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
```

Verifique que el nuevo certificado esté instalado:

```
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
```

Nota: Los certificados autofirmados caducan a las 00:00 1 de enero de 2020 UTC y no podrá crearlos después de ese momento.

Preguntas y respuestas

A: ¿Cuál es el problema?

Los certificados PKI X.509 autofirmados generados en productos que ejecutan versiones de Cisco IOS o Cisco IOS XE afectadas caducan el 01/01/2020 00:00:00 UTC. Los nuevos certificados autofirmados no se pueden crear en los dispositivos afectados después del 01/01/2020 00:00:00 UTC. Cualquier servicio que se base en estos certificados autofirmados ya no puede funcionar después de que caduque el certificado.

A: ¿Cuál es el impacto en la red de un cliente si caduca un certificado autofirmado para su producto?

La funcionalidad de cualquier producto afectado que se base en los certificados autofirmados ya no puede funcionar después de que caduque el certificado. Consulte el aviso relevante para obtener más información.

A: ¿Cómo puedo saber si me afecta este problema?

El aviso práctico proporciona instrucciones para determinar si utiliza un certificado autofirmado y si esta incidencia afecta a su configuración. Consulte la sección "Cómo identificar los productos afectados" en el aviso práctico.

A: ¿Hay algún guión que pueda ejecutar para ver si me afecta?

Yes. Utilice el Analizador de Cisco CLI, ejecute un Diagnóstico del sistema. Si el certificado está presente y se utiliza, se puede mostrar una alerta. https://cway.cisco.com/cli/

P. ¿Ha proporcionado Cisco soluciones de software para este problema?

Yes. Cisco ha publicado soluciones de software para este problema, así como soluciones alternativas en caso de que una actualización de software no sea factible inmediatamente. Consulte el aviso práctico para obtener más información.

A: ¿Este problema afecta a algún producto de Cisco que utilice un certificado?

No. Este problema afecta **sólo a los productos que utilizan certificados autofirmados generados por versiones específicas de Cisco IOS o Cisco IOS XE** con el certificado aplicado a un servicio del producto. Este problema no afecta a los productos que utilizan certificados generados por una entidad emisora de certificados (CA).

A: ¿Los productos de Cisco utilizan solo certificados autofirmados?

No. Los certificados pueden ser generados por una autoridad de certificación externa de terceros o en el propio dispositivo Cisco IOS o Cisco IOS XE como certificado autofirmado. Los requisitos específicos del usuario pueden requerir el uso de certificados autofirmados. Este problema no afecta a los certificados generados por una entidad emisora de certificados (CA).

P. ¿Por qué ocurrió este problema?

Desafortunadamente, a pesar de los esfuerzos de los proveedores de tecnología, los defectos de software siguen ocurriendo. Cuando se descubre un error en cualquier tecnología de Cisco, estamos comprometidos con la transparencia y con proporcionar a nuestros usuarios la información que necesitan para proteger su red.

En este caso, el problema se debe a un error de software conocido en el que las versiones afectadas de Cisco IOS y Cisco IOS XE siempre pueden establecer la fecha de vencimiento del certificado autofirmado en 01/01/2020 00:00:00 UTC. Después de esta fecha, el certificado caduca y no es válido, lo que podría afectar a la funcionalidad del producto.

A: ¿Por qué se ha elegido una fecha de caducidad del 1 de enero de 2020 00:00:00 UTC?

Los certificados suelen tener una fecha de caducidad. En el caso de este error de software, la fecha del 1 de enero de 2020 se utilizó durante el desarrollo del software Cisco IOS y Cisco IOS XE hace más de 10 años y es un error humano.

A: ¿Qué productos se ven afectados por este problema?

Cualquier producto de Cisco que ejecute las versiones de Cisco IOS anteriores a 15.6(03)M07, 15.7(03)M05, 15.8(03)M03 y 15.9(03)M y cualquier producto de Cisco que ejecute las versiones de Cisco IOS XE anteriores a 16.9.1

A: ¿Qué deben hacer los usuarios?

Debe revisar el aviso de campo para evaluar si este problema le afecta y, en caso afirmativo, seguir las instrucciones de la solución o solución alternativa para mitigarlo.

A: ¿Es este problema una vulnerabilidad de seguridad?

No. No se trata de una vulnerabilidad de seguridad y no hay riesgo para la integridad del producto.

A: ¿Se ve afectado SSH?

No. SSH utiliza pares de claves RSA pero no utiliza certificados excepto en una configuración poco común. Para que Cisco IOS utilice certificados, debe estar presente la siguiente configuración.

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

A: ¿Qué versiones fijas están disponibles para las plataformas Catalyst 2K, 3K, 4K y 6K clásicas?

Para plataformas basadas en Polaris (3650/3850/Catalyst 9K series), la corrección está disponible a partir de la versión 16.9.1
Para la plataforma CDB, fix está disponible a partir de la versión 15.2(7)E1a

Para las demás plataformas de switching clásicas:

Las confirmaciones están en curso pero no hemos publicado la versión de CCO. La próxima versión de CCO puede tener la solución.

Entre tanto, utilice una de las otras soluciones alternativas disponibles.

A: ¿Se ve afectado WAAS?

WAAS sigue funcionando correctamente y optimizando el tráfico; sin embargo, AppNav-XE y Central Manager se desconectaron para conectarse al dispositivo que tiene un certificado autofirmado caducado. Esto significa que no puede supervisar AppNav-Cluster ni cambiar ninguna política para WAAS. En resumen, WAAS sigue funcionando correctamente, pero la gestión y la supervisión se suspenden hasta que se resuelve el problema del certificado. Para resolver el problema, puede que sea necesario generar un nuevo certificado en Cisco IOS y luego importarlo a Central Manager.

Información Relacionada

- Consulte FN70489 Field Notice: FN - 70489 - Vencimiento del certificado autofirmado PKI en Cisco IOS y Cisco IOS XE Software
- Consulte ID de bug de Cisco CSCvi48253

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).