Vencimento do certificado autoassinado IOS em 1º de janeiro de 2020

Contents

Introduction

Este documento descreve os efeitos e erros causados pela expiração dos certificados autoassinados (SSC) nos sistemas de software da Cisco e fornece várias soluções.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Certificados com assinatura automática (SSC)
- Cisco IOS® versão 12.x e posterior

Componentes Utilizados

Os componentes são os sistemas de software afetados pela expiração do SSC.

Todos os sistemas Cisco IOS e Cisco IOS® XE que usam um certificado autoassinado, que não têm a correção de bug da Cisco ID CSCvi48253 ou que não tinham a correção de bug da Cisco ID CSCvi48253 quando o SSC foi gerado. Isso inclui:

- Todos os Cisco IOS 12.x
- Todos os Cisco IOS 15.x anteriores a 15.6(3)M7, 15.7(3)M5, 15.8(3)M3, 15.9(3)M
- Todos os 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Background

> **Note**: Este documento contém o conteúdo de FN40789 , juntamente com contexto adicional, exemplos, atualizações e Perguntas e Respostas.

Às 00:00 do dia 1º de janeiro de 2020 UTC, todos os certificados autoassinados (SSC) gerados nos sistemas Cisco IOS e Cisco IOS XE foram definidos para expirar, a menos que o sistema executasse uma versão fixa do Cisco IOS e Cisco IOS XE quando o SSC fosse gerado. Após esse período, os sistemas Cisco IOS não fixos não poderão gerar novos SSCs. Qualquer serviço que dependa desses certificados autoassinados para estabelecer ou encerrar uma conexão segura não funcionará depois que o certificado expirar.

Esse problema afeta apenas os certificados com assinatura automática que foram gerados pelo dispositivo Cisco IOS ou Cisco IOS XE e aplicados a um serviço no dispositivo. Os certificados que foram gerados por uma Autoridade de Certificação (CA), que inclui os certificados gerados pelo recurso Cisco IOS CA, não são afetados por esse problema.

Certos recursos do software Cisco IOS e Cisco IOS XE dependem de certificados X.509 assinados digitalmente para validação de identidade criptográfica. Esses certificados são gerados por uma CA externa de terceiros ou no próprio dispositivo Cisco IOS ou Cisco IOS XE como um certificado autoassinado. As versões do software Cisco IOS e Cisco IOS XE afetadas definem a data de expiração do certificado autoassinado como 2020-01-01 00:00:00 UTC. Após essa data, o certificado expira e é inválido.

Os serviços que podem confiar em um certificado autoassinado incluem:

Recursos gerais

- Servidor HTTP sobre TLS (HTTPS) - O HTTPS produz um erro no navegador que indica que o certificado expirou.
- Servidor SSH - Os usuários que usam certificados X.509 para autenticar a sessão SSH podem falhar na autenticação. (O uso de certificados X.509 é raro. A autenticação de nome de usuário/senha e a autenticação de chave pública/privada não são afetadas.)
- RESTCONF - As conexões RESTCONF podem falhar.

Recursos de colaboração

- Protocolo de Iniciação de Sessão (SIP - Session Initiation Protocol) sobre TLS
- Cisco Unified Communications Manager Express (CME) com sinalização criptografada ativada
- Cisco Unified Survivable Remote Site Telephony (SRST) com sinalização criptografada habilitada
- Cisco IOS dspfarm recursos (Conferência, Media Termination Point ou Transcodificação) com sinalização criptografada ativada
- Portas Skinny Client Control Protocol (SCCP) Telephony Control Application (STCAPP) configuradas com sinalização criptografada
- Protocolo de Controle de Gateway de Mídia (MGCP - Media Gateway Control Protocol) e sinalização de chamada H.323 sobre segurança IP (IPSec - Signaling over IP Security) sem uma chave pré-compartilhada
- API de serviços do Cisco Unified Communications Gateway no modo seguro (que usa HTTPS)

Recursos sem fio

- Conexões LWAPP/CAPWAP entre pontos de acesso Cisco IOS mais antigos (fabricados em 2005 ou antes) e Wireless LAN Controller. Consulte o Field Notice da Cisco FN63942 para obter mais detalhes.

Problema

Uma tentativa de gerar um certificado autoassinado em um Cisco IOS ou Cisco IOS XE Software Release afetado após 2020-01-01 00:00:00 UTC resulta neste erro:

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

Os serviços que dependem do certificado autoassinado não funcionam. Por exemplo:

- As chamadas SIP sobre TLS não são concluídas.
- Os dispositivos registrados no Cisco Unified CME com sinalização criptografada ativada não funcionam mais.
- O Cisco Unified SRST com sinalização criptografada ativada não permite que os dispositivos

sejam registrados.
- Os recursos dspfarm do Cisco IOS (Conferência, Media Termination Point ou Transcodificação) com sinalização criptografada ativada não são mais registrados.
- As portas STCAPP configuradas com sinalização criptografada não são mais registradas.
- As chamadas através de um gateway que o MGCP ou a sinalização de chamada H.323 sobre IPSec sem uma chave pré-compartilhada podem falhar.
- As chamadas de API que usam a API de serviços do Cisco Unified Communications Gateway Services no modo seguro (que usam HTTPS) podem falhar.
- RESTCONF pode falhar.
- As sessões HTTPS para gerenciar o dispositivo exibem um aviso do navegador, que indica que o certificado expirou.
- As sessões do AnyConnect SSL VPN não conseguem estabelecer ou relatar um certificado inválido.
- As conexões IPSec podem falhar ao serem estabelecidas.

Como identificar produtos afetados

> **Note**: Para ser afetado por este aviso de campo, um dispositivo deve ter um certificado autoassinado definido *e* o certificado autoassinado deve ser aplicado a um ou mais recursos conforme descrito abaixo. A presença de um certificado autoassinado sozinho não afeta a operação do dispositivo quando o certificado expira e não requer ação imediata. **Para ser afetado, um dispositivo deve atender aos critérios das etapas 3 e 4 abaixo.**

Para determinar se você usa um certificado autoassinado:

1. Digite o `show running-config | begin crypto` no dispositivo.
2. Procure a configuração de ponto de confiança crypto PKI.
3. Na configuração de ponto de confiança de criptografia PKI, procure a configuração de registro de ponto de confiança. A inscrição de ponto de confiança deve ser configurada para que " **autoassinado**" seja afetado. Além disso, o certificado autoassinado também deve aparecer na configuração. Observe que o nome do ponto de confiança não contém as palavras "autoassinado" como mostrado neste próximo exemplo.

```
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
```

   Se o registro de ponto de confiança *não* **estiver configurado para** "autoassinado"; **o dispositivo NÃO será afetado por este field notice**. Nenhuma ação é exigida.Se a inscrição de ponto de confiança *estiver* **configurada para "autoassinado" e se o Certificado Autoassinado aparecer na configuração, o dispositivo de poderá ser afetado por este aviso de campo.** continuar na etapa 4.
4. Se você determinou na Etapa 3 que a inscrição de ponto de confiança está configurada para "autoassinado" e que o certificado autoassinado aparece na configuração, verifique se o

certificado autoassinado está aplicado a um recurso no dispositivo.Vários recursos que podem ser vinculados ao SSC são mostrados nestes exemplos de configuração:

- Para o **servidor HTTPS**, este texto deve estar presente:

```
ip http secure-server
```

Além disso, um ponto de confiança também pode ser definido como mostrado no próximo exemplo de código. Se esse comando não estiver presente, o comportamento padrão será usar o certificado autoassinado.

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

Se um ponto de confiança for definido e apontar para um certificado diferente do certificado autoassinado, você não será afetado.

Para o **servidor HTTPS**, o impacto do certificado expirado é menor porque os certificados autoassinados já não são confiáveis para navegadores da Web e geram um aviso mesmo quando não estão expirados. A presença de um certificado expirado pode alterar o aviso que você recebe no navegador.

- Para **SIP sobre TLS**, este texto está presente no arquivo de configuração:

```
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 o **Cisco Unified CME** com sinalização criptografada ativada, este texto está presente no arquivo de configuração:

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

- Para o **Cisco Unified SRST** com sinalização criptografada ativada, este texto está presente no arquivo de configuração:

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

- Para **Cisco IOS dspfarm recursos** (Conference, Media Termination Point ou Transcoding) com a sinalização criptografada ativada, este texto estará presente no arquivo de configuração:

```
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 **portas STCAPP** configuradas com sinalização criptografada, este texto está presente no arquivo de configuração:
```
stcapp security trust-point <self-signed-trust-point-name>
stcapp security mode encrypted
```
- Para a **API de serviços do Cisco Unified Communications Gateway Services no modo seguro**, este texto está presente no arquivo de configuração:
```
uc secure-wsapi
ip http secure-server
ip http secure-trust-point TP-self-signed-XXXXXXXX
```
- Para **SSLVPN**, este texto está presente no arquivo de configuração:
```
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**, o certificado autoassinado pode ser usado se qualquer uma das configurações estiver presente (uma análise adicional da configuração é necessária para determinar se o recurso usa o certificado autoassinado versus um 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 o **servidor SSH**, é extremamente improvável que você possa aproveitar certificados para autenticar as sessões SSH. No entanto, você pode verificar sua configuração para verificar isso. Você deve ter todas as três linhas exibidas no próximo exemplo de código para ser afetado. **Note**: Se você aproveitou a combinação de nome de usuário e senha para SSH em seu dispositivo, então você NÃO é afetado.
```
ip ssh server certificate profile
 ! Certificate used by server
 server
  trust-point sign TP-self-signed-xxxxxx
```
- Para **RESTCONF**, este texto está presente no arquivo de configuração:
```
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
```

Solução(ões)

A solução é atualizar o software Cisco IOS ou Cisco IOS XE para uma versão que inclua a correção:

- Software Cisco IOS XE versão 16.9.1 e posterior
- Software Cisco IOS versão 15.6(3)M7 e posterior; 15.7(3)M5 e posterior; ou 15.8(3)M3 e posterior

Depois de atualizar o software, você deve regenerar o certificado autoassinado e exportá-lo para

qualquer dispositivo que possa exigir o certificado em seu armazenamento confiável.

Três alternativas estão disponíveis se uma atualização imediata de software não for viável:

1. Obtenha um certificado válido de uma Autoridade de Certificação (CA) de terceiros.
2. Use o Cisco IOS CA Server para gerar um novo certificado.
3. Use o OpenSSL para gerar um novo certificado autoassinado.

1. Obter um Certificado Válido de uma Autoridade de Certificação (CA) de terceiros

Instalar um certificado de uma autoridade de certificação. As CAs comuns incluem: Comodo Let's Criptografe, RapidSSL, Thawte, Sectigo, GeoTrust, Symantec e assim por diante. Com essa solução, uma solicitação de certificado é gerada e exibida pelo Cisco IOS. Em seguida, o administrador copia a solicitação, a envia para uma CA de terceiros e recupera o resultado.

> **Note**: O uso de uma CA para assinar certificados é considerado uma prática recomendada de segurança. Este procedimento é fornecido como uma solução neste aviso de campo; no entanto, é preferível continuar a usar o certificado assinado por CA de terceiros depois de aplicar esta solução alternativa, em vez de usar um certificado autoassinado.

Para instalar um certificado de uma CA de terceiros:

1. Criar uma CSR (Solicitação de Assinatura de Certificado):

```
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. Envie o CSR à CA de terceiros.**Note**: O procedimento para enviar o CSR a uma CA de terceiros e recuperar o certificado resultante varia de acordo com a CA usada. Consulte a documentação do CA para obter instruções sobre como executar esta etapa.
2. Baixe o novo certificado de identidade para o roteador junto com o certificado CA.
3. Instale o certificado CA no 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 o certificado de identidade no 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. Usar o Cisco IOS CA Server para Gerar um Novo Certificado

Use o servidor Cisco IOS Certificate Authority local para gerar e assinar um novo certificado.

Nota:O recurso de servidor de CA local não está disponível em todos os produtos.

```
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. Usar o OpenSSL para Gerar um Novo Certificado Autoassinado

Use o OpenSSL para gerar um pacote de certificados PKCS12 e importar o pacote para o Cisco IOS.

Exemplo de 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
```

Exemplo de roteador 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
```

Verifique se o novo certificado está 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
```

> **Note**: Os certificados autoassinados expiram às 00:00 1º de janeiro de 2020 UTC e não poderão ser criados depois dessa data.

Perguntas e respostas

P: Que é o problema?

Os certificados X.509 PKI autoassinados gerados em produtos que executam as versões afetadas do Cisco IOS ou do Cisco IOS XE expiram em 01/01/2020 00:00:00 UTC. Novos certificados com assinatura automática não podem ser criados nos dispositivos afetados após 01/01/2020 00:00:00 UTC. Qualquer serviço que dependa desses certificados autoassinados não poderá mais funcionar após a expiração do certificado.

P: Qual será o impacto para uma rede de cliente se um certificado autoassinado expirar para seu produto?

Qualquer funcionalidade do produto afetado que dependa dos certificados autoassinados não poderá mais funcionar após a expiração do certificado. Consulte o aviso de campo para obter mais detalhes.

P: Como posso saber se fui afetado por esse problema?

O Field Notice fornece instruções para determinar se você usa um Certificado Autoassinado e se sua configuração é afetada por esse problema. Consulte a seção "Como identificar produtos afetados" no Field Notice.

P: Há um script que eu possa executar para ver se fui afetado?

Yes. Use o Cisco CLI Analyzer, execute um diagnóstico de sistema. Se o certificado estiver presente e for usado, um alerta poderá ser exibido. https://cway.cisco.com/cli/

P. A Cisco forneceu correções de software para esse problema?

Yes. A Cisco lançou correções de software para esse problema, bem como soluções caso uma atualização de software não seja imediatamente viável. Consulte o Field Notice para obter detalhes completos.

P: Esse problema afeta algum produto da Cisco que usa um certificado?

Não. Esse problema afeta **somente produtos que usam certificados com assinatura automática gerados por versões específicas do Cisco IOS ou Cisco IOS XE** com o certificado aplicado a um

serviço no produto. Os produtos que usam certificados gerados por uma autoridade de certificação (CA) não são afetados por esse problema.

P: Os produtos da Cisco usam apenas certificados com assinatura automática?

Não. Os certificados podem ser gerados por uma autoridade de certificação externa de terceiros ou no próprio dispositivo Cisco IOS ou Cisco IOS XE como um certificado autoassinado. Os requisitos específicos do usuário podem exigir o uso de certificados com assinatura automática. Os certificados gerados por uma autoridade de certificação (CA) não são afetados por esse problema.

P. Por que esse problema ocorreu?

Infelizmente, apesar dos melhores esforços dos fornecedores de tecnologia, ainda ocorrem defeitos de software. Quando um bug é descoberto em qualquer tecnologia da Cisco, temos o compromisso de transparência e fornecer aos nossos usuários as informações necessárias para proteger sua rede.

Nesse caso, o problema é causado por um bug de software conhecido no qual as versões afetadas do Cisco IOS e do Cisco IOS XE sempre podem definir a data de expiração do certificado autoassinado como 01/01/2020 00:00:00 UTC. Após essa data, o certificado expira e é inválido, o que pode afetar a funcionalidade do produto.

P: Por que foi escolhida a data de vencimento de 1º de janeiro de 2020 00:00:00 UTC?

Os certificados normalmente têm uma data de expiração. No caso desse bug de software, a data de 1º de janeiro de 2020 foi usada durante o desenvolvimento do software Cisco IOS e Cisco IOS XE há mais de 10 anos e é um erro humano.

P: Quais produtos são afetados por esse problema?

Qualquer produto da Cisco que execute versões do Cisco IOS anteriores a 15.6(03)M07, 15.7(03)M05, 15.8(03)M03 e 15.9(03)M e qualquer produto da Cisco que execute versões do Cisco IOS XE anteriores a 16.9.1

P: O que os usuários precisam fazer?

Você precisa revisar o aviso de campo para avaliar se o problema o afeta e, se for o caso, seguir as instruções de Solução alternativa para atenuar o problema.

P: Esse problema é uma vulnerabilidade de segurança?

Não. Essa não é uma vulnerabilidade de segurança e não há risco para a integridade do produto.

P: O SSH é afetado?

Não. O SSH usa pares de chaves RSA, mas não utiliza certificados, exceto em uma configuração rara. Para que o Cisco IOS utilize certificados, a próxima configuração deve estar presente.

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

P: Quais versões fixas estão disponíveis para as plataformas Classic Catalyst 2K, 3K, 4K e 6K?

Para plataformas baseadas em Polaris (série 3650/3850/Catalyst 9K), a correção está disponível a partir da versão 16.9.1
Para a plataforma CDB, a correção está disponível a partir da versão 15.2(7)E1a

Para as outras plataformas de comutação clássicas:

As confirmações estão em andamento, mas não publicamos a versão do CCO. A próxima versão do CCO pode ter a correção.

No período, utilize uma das outras soluções disponíveis.

P: O WAAS é afetado?

O WAAS continua a operar corretamente e otimizar o tráfego, no entanto, o AppNav-XE e o Central Manager ficaram offline para o dispositivo que tem um certificado autoassinado expirado. Isso significa que você não pode monitorar AppNav-Cluster ou alterar qualquer política para WAAS. Em resumo, o WAAS continua funcionando corretamente, mas o gerenciamento e o monitoramento são suspensos até que o problema do certificado seja resolvido. Para resolver o problema, um novo certificado pode precisar ser gerado no Cisco IOS e importado para o Central Manager.

Informações Relacionadas

- Consulte Nota de campo FN70489: FN - 70489 - Expiração do Certificado Autosassinado PKI no Cisco IOS e no Cisco IOS XE Software
- Consulte o bug da Cisco ID CSCvi48253

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.