Scadenza certificato autofirmato IOS il 1° gennaio 2020

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Sfondo
Caratteristiche generali
Funzioni di collaborazione
Funzioni wireless
Problema
Come identificare i prodotti interessati
Soluzione/i
1. Ottenere un certificato valido da un'autorità di certificazione (CA) di terze parti
2. Utilizzare il server CA Cisco IOS per generare un nuovo certificato
Esempio di router Cisco IOS o Cisco IOS XE
Domande e risposte
D: Qual è il problema?
D: Qual è l'impatto per una rete client se un certificato autofirmato scade per il prodotto?
D: Come è possibile stabilire se il problema si verifica?
D: Esiste uno script che è possibile eseguire per verificare se il problema si verifica?
D. Cisco ha fornito soluzioni software per questo problema?
D: Il problema riguarda tutti i prodotti Cisco che utilizzano un certificato?
D: I prodotti Cisco utilizzano solo certificati autofirmati?
D. Perché si è verificato questo problema?
D: Perché è stata scelta una data di scadenza 1 gennaio 2020 00:00:00 UTC?
D: Quali prodotti sono interessati da questo problema?
D: Cosa devono fare gli utenti?
D: Si tratta di un problema di sicurezza?
D: Il protocollo SSH è interessato?
D: Quali versioni fisse sono disponibili per le piattaforme Classic Catalyst 2K, 3K, 4K, 6K?
D: Il problema è WAAS?
Informazioni correlate

Introduzione

Questo documento descrive gli effetti e gli errori causati dalla scadenza dei Certificati autofirmati (SSC) sui sistemi software Cisco e fornisce diverse soluzioni.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Certificati autofirmati (SSC)
- Cisco IOS® versione 12.x e successive

Componenti usati

I componenti sono i sistemi software interessati dalla scadenza del SSC.

Tutti i sistemi Cisco IOS e Cisco IOS® XE che utilizzano un certificato autofirmato, non dispongono dell'ID bug Cisco CSCvi48253 corretto o non dispongono della correzione dell'ID bug Cisco CSCvi48253 al momento della generazione del certificato SSC. Ciò include:

- Tutto Cisco IOS 12.x
- Tutti i Cisco IOS 15.x con versione precedente a 15.6(3)M7, 15.7(3)M5, 15.8(3)M3, 15.9(3)M
- Tutti i Cisco IOS XE precedenti alla 16.9.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Sfondo

> **Nota:** Questo documento contiene i contenuti di FN40789 e ulteriori informazioni su contesto, esempi, aggiornamenti e domande e risposte.

Alle 00:00 del 1° gennaio 2020 UTC, tutti i certificati autofirmati (SSC) generati sui sistemi Cisco IOS e Cisco IOS XE erano impostati per scadere, a meno che il sistema non eseguisse una versione fissa di Cisco IOS e Cisco IOS XE quando è stato generato il SSC. Trascorso questo periodo, i sistemi Cisco IOS non fissi non saranno in grado di generare nuovi SSC. I servizi che utilizzano questi certificati autofirmati per stabilire o terminare una connessione protetta non funzionano dopo la scadenza del certificato.

Questo problema riguarda solo i certificati autofirmati che sono stati generati dal dispositivo Cisco IOS o Cisco IOS XE e applicati a un servizio sul dispositivo. Il problema non interessa i certificati generati da un'Autorità di certificazione (CA), inclusi i certificati generati dalla funzionalità CA di Cisco IOS.

Alcune funzionalità dei software Cisco IOS e Cisco IOS XE si basano su certificati X.509 con firma digitale per la convalida dell'identità crittografica. Questi certificati possono essere generati da un'autorità di certificazione esterna di terze parti o sul dispositivo Cisco IOS o Cisco IOS XE stesso come certificato autofirmato. Le versioni software Cisco IOS e Cisco IOS XE interessate impostano la data di scadenza del certificato autofirmato su 2020-01-01 00:00:00 UTC. Dopo questa data, il certificato scade e non è valido.

I servizi che possono fare affidamento su un certificato autofirmato includono:

Caratteristiche generali

- Server HTTP su TLS (HTTPS) - HTTPS genera un errore nel browser che indica che il certificato è scaduto.
- Server SSH: l'autenticazione degli utenti che usano i certificati X.509 per autenticare la sessione SSH può non riuscire. L'utilizzo di certificati X.509 è raro. l'autenticazione di nome utente/password e l'autenticazione con chiave pubblica/privata non sono interessate).
- RESTCONF - Le connessioni RESTCONF possono non riuscire.

Funzioni di collaborazione

- Session Initiation Protocol (SIP) over TLS
- Cisco Unified Communications Manager Express (CME) con segnalazione crittografata abilitata
- Cisco Unified Survivable Remote Site Telephony (SRST) con segnalazione crittografata abilitata
- Cisco IOS dspfarm risorse (conferenza, punto di terminazione multimediale o transcodifica) con segnalazione crittografata abilitata
- Porte STCAPP (Telephony Control Application) SCCP (Skinny Client Control Protocol) configurate con segnalazione crittografata
- MGCP (Media Gateway Control Protocol) e IPSec (Call Signaling over IP Security) H.323 senza una chiave già condivisa
- API dei servizi gateway di Cisco Unified Communications in modalità protetta (che utilizza HTTPS)

Funzioni wireless

- Connessioni LWAPP/CAPWAP tra i precedenti punti di accesso Cisco IOS (prodotti nel 2005 o versioni precedenti) e Wireless LAN Controller. Per ulteriori informazioni, vedere la notifica sul campo FN63942 di Cisco.

Problema

Un tentativo di generare un certificato autofirmato su una versione del software Cisco IOS o Cisco IOS XE interessata dopo l'ora UTC 2020-01-01 00:00:00 ha come risultato questo errore:

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

I servizi che si basano sul certificato autofirmato non funzionano. Ad esempio:

- Chiamate SIP over TLS non completate.
- I dispositivi registrati su Cisco Unified CME con segnalazione crittografata abilitata non funzionano più.
- Cisco Unified SRST con segnalazione crittografata abilitata non consente ai dispositivi di registrarsi.
- Le risorse dspfarm Cisco IOS (conferenza, punto di terminazione multimediale o transcodifica) con segnalazione crittografata abilitata non possono più essere registrate.

- Le porte STCAPP configurate con la segnalazione crittografata non si registrano più.
- Le chiamate tramite un gateway che supportano la segnalazione delle chiamate MGCP o H.323 su IPSec senza una chiave precondivisa possono non riuscire.
- Le chiamate API che utilizzano l'API dei servizi gateway di Cisco Unified Communications in modalità protetta (che utilizza HTTPS) possono avere esito negativo.
- RESTCONF può non riuscire.
- Le sessioni HTTPS per la gestione del dispositivo visualizzano un avviso del browser che indica che il certificato è scaduto.
- Sessioni VPN SSL di AnyConnect: impossibile stabilire o segnalare un certificato non valido.
- Èpossibile che le connessioni IPSec non vengano stabilite correttamente.

Come identificare i prodotti interessati

> **Nota:** Per essere interessati da questo avviso di campo, è necessario che per un dispositivo sia definito un certificato autofirmato *e che* il certificato autofirmato sia applicato a una o più funzionalità descritte di seguito. La presenza di un solo certificato autofirmato non influisce sul funzionamento del dispositivo alla scadenza del certificato e non richiede un'azione immediata. **Per essere interessati, un dispositivo deve soddisfare i criteri sia al punto 3 che al punto 4.**

Per determinare se si utilizza un certificato autofirmato:

1. Immettere il show running-config | begin crypto sul dispositivo.
2. Cercare la configurazione del trust point PKI di crittografia.
3. Nella configurazione del trust point PKI di crittografia cercare la configurazione della registrazione del trust point. Affinché l'operazione abbia effetto, è necessario configurare la registrazione del trust point. Nella configurazione deve inoltre essere visualizzato il certificato autofirmato. Si noti che il nome del trust point non contiene le parole "self-signed", come illustrato nell'esempio seguente.

```
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 la registrazione del trust point *non* è configurata per "selfsigned", **il dispositivo NON è interessato da questo avviso di campo**. Non sono necessarie ulteriori azioni.**Se la registrazione del punto di attendibilità *è* configurata per "self-signed" e il certificato autofirmato viene visualizzato nella configurazione**; il **dispositivo può essere interessato** da questo avviso di campo. Passare al punto 4.
4. Se nel passaggio 3 è stato determinato che la registrazione del punto di attendibilità è configurata per "self-signed" e che il certificato autofirmato viene visualizzato nella configurazione, verificare se il certificato autofirmato è applicato a una funzionalità nel dispositivo.Di seguito sono riportate alcune funzioni che possono essere collegate al SSC:

- Per il **server HTTPS**, il testo deve essere presente:

```
ip http secure-server
```

Èinoltre possibile definire un trust point come illustrato nell'esempio di codice seguente. Se questo comando non è presente, per impostazione predefinita viene utilizzato il certificato autofirmato.

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

La definizione di un trust point che punta a un certificato diverso dal certificato autofirmato non influisce sull'utente.

Per il **server HTTPS**, l'impatto del certificato scaduto è minimo perché i certificati autofirmati sono già considerati non attendibili dai browser Web e generano un avviso anche quando non sono scaduti. La presenza di un certificato scaduto può modificare l'avviso visualizzato nel browser.

- Per **SIP over TLS**, questo testo è presente nel file di configurazione:

```
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>
!
```

- Per **Cisco Unified CME** con segnalazione crittografata abilitata, questo testo è presente nel file di configurazione:

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

- Per **Cisco Unified SRST** con segnalazione crittografata abilitata, questo testo è presente nel file di configurazione:

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

- Per **Cisco IOS dspfarm risorsa**s (Conference, Media Termination Point, o Transcoding) con la segnalazione crittografata abilitata, questo testo è presente nel file di configurazione:

```
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>
!
```

- Per **le porte STCAPP** configurate con segnalazione crittografata, questo testo è presente nel file di configurazione:

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

- Per l'**API dei servizi gateway di Cisco Unified Communications in modalità protetta**, questo testo è presente nel file di configurazione:

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

- Per **SSLVPN**, questo testo è presente nel file di configurazione:

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

OR

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

- Per **ISAKMP e IKEv2**, è possibile utilizzare il certificato autofirmato se è presente una qualsiasi delle configurazioni (è necessaria un'ulteriore analisi della configurazione per determinare se la funzionalità utilizza il certificato autofirmato rispetto a un certificato diverso):

```
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
```

- Per il **server SSH**, è estremamente improbabile che si possano usare i certificati per autenticare le sessioni SSH. Tuttavia, è possibile controllare la configurazione per verificare questa condizione. Per essere interessati, è necessario che nel codice di esempio riportato di seguito siano visualizzate tutte e tre le righe. **Nota:** L'uso combinato di nome utente e password per il protocollo SSH sul dispositivo NON comporta alcun impatto sull'utente.

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

- Per **RESTCONF**, questo testo è presente nel file di configurazione:

```
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
```

Soluzione/i

La soluzione è aggiornare il software Cisco IOS o Cisco IOS XE a una versione che includa la correzione:

- Software Cisco IOS XE release 16.9.1 e successive
- Software Cisco IOS release 15.6(3)M7 e successive; 15.7(3)M5 e successive; o 15.8(3)M3 e versioni successive

Dopo aver aggiornato il software, è necessario rigenerare il certificato autofirmato ed esportarlo in qualsiasi dispositivo che possa richiedere il certificato nel relativo archivio attendibile.

Se non è possibile un aggiornamento immediato del software, sono disponibili tre soluzioni:

1. Ottenere un certificato valido da un'Autorità di certificazione (CA) di terze parti.

2. Utilizzare il server CA Cisco IOS per generare un nuovo certificato.
3. Utilizzare OpenSSL per generare un nuovo certificato autofirmato.

1. Ottenere un certificato valido da un'autorità di certificazione (CA) di terze parti

Installare un certificato da un'autorità di certificazione. Le CA comuni includono: Comodo Let's Encrypt, RapidSSL, Thawte, Sectigo, GeoTrust, Symantec e così via. Con questa soluzione, Cisco IOS genera e visualizza una richiesta di certificato. L'amministratore quindi copia la richiesta, la invia a un'autorità di certificazione di terze parti e recupera il risultato.

> **Nota:** L'utilizzo di una CA per firmare i certificati è considerato una procedura consigliata per la sicurezza. Questa procedura viene fornita come soluzione in questo avviso sul campo; tuttavia, è preferibile continuare a utilizzare il certificato firmato dall'autorità di certificazione di terze parti dopo aver applicato questa soluzione, anziché utilizzare un certificato autofirmato.

Per installare un certificato da una CA di terze parti:

1. Creare una richiesta di firma del certificato (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. Inviare il CSR all'autorità di certificazione di terze parti.**Nota:** La procedura per inviare il CSR a un'autorità di certificazione di terze parti e recuperare il certificato il cui risultato varia in base all'autorità di certificazione utilizzata. Per istruzioni su come eseguire questo passaggio, consultare la documentazione della CA.
2. Scaricare il nuovo certificato di identità per il router insieme al certificato CA.
3. Installare il certificato CA nel 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. Installare il certificato di identità nel 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. Utilizzare il server CA Cisco IOS per generare un nuovo certificato

Utilizzare il server Cisco IOS Certificate Authority locale per generare e firmare un nuovo certificato.

> **Nota**:la funzionalità server CA locale non è disponibile su tutti i prodotti.

```
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. Utilizzare OpenSSL per generare un nuovo certificato autofirmato

Utilizzare OpenSSL per generare un pacchetto di certificati PKCS12 e importare il pacchetto in Cisco IOS.

Esempio di 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
```

Esempio di 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
```

Verificare che il nuovo certificato sia installato:

```
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: I certificati autofirmati scadono il 00:00 1 gen 2020 UTC e non è possibile crearli dopo tale data.

Domande e risposte

D: Qual è il problema?

I certificati PKI X.509 autofirmati generati su prodotti che eseguono le versioni interessate di Cisco IOS o Cisco IOS XE scadono il 01/01/2020 00:00:00 UTC. Impossibile creare nuovi certificati autofirmati sui dispositivi interessati dopo le ore 01/01/2020 00:00:00 UTC. Tutti i servizi basati su questi certificati autofirmati non potranno più funzionare dopo la scadenza del certificato.

D: Qual è l'impatto per una rete client se un certificato autofirmato scade per il prodotto?

Le funzionalità del prodotto interessato che si basano sui certificati autofirmati non possono più funzionare dopo la scadenza del certificato. Per ulteriori informazioni, vedere l'avviso sui prodotti.

D: Come è possibile stabilire se il problema si verifica?

La notifica sul campo fornisce istruzioni per determinare se si utilizza un certificato autofirmato e se la configurazione è interessata da questo problema. Consulta la sezione "Come identificare i prodotti interessati" nell'avviso sui prodotti.

D: Esiste uno script che è possibile eseguire per verificare se il problema si verifica?

Sì. Usare Cisco CLI Analyzer, eseguire Diagnostica sistema. Se il certificato è presente e viene utilizzato, è possibile visualizzare un avviso. https://cway.cisco.com/cli/

D. Cisco ha fornito soluzioni software per questo problema?

Sì. Cisco ha rilasciato le correzioni software per questo problema e le soluzioni da adottare nel caso in cui non sia possibile aggiornare il software immediatamente. Per informazioni dettagliate, consultare la Notifica.

D: Il problema riguarda tutti i prodotti Cisco che utilizzano un certificato?

No. Questo problema riguarda **solo i prodotti che utilizzano certificati autofirmati generati da versioni specifiche di Cisco IOS o Cisco IOS XE** con il certificato applicato a un servizio sul prodotto. Il problema non interessa i prodotti che utilizzano certificati generati da un'Autorità di certificazione (CA).

D: I prodotti Cisco utilizzano solo certificati autofirmati?

No. I certificati possono essere generati da un'autorità di certificazione esterna di terze parti o sul dispositivo Cisco IOS o Cisco IOS XE stesso come certificato autofirmato. L'utilizzo di certificati autofirmati può richiedere requisiti utente specifici. Il problema non interessa i certificati generati da un'Autorità di certificazione (CA).

D. Perché si è verificato questo problema?

Purtroppo, nonostante gli sforzi dei fornitori di tecnologia, i difetti del software continuano a verificarsi. Quando si scopre un bug in una tecnologia Cisco, ci impegniamo a garantire la trasparenza e a fornire ai nostri utenti le informazioni di cui hanno bisogno per proteggere la loro rete.

In questo caso, il problema è causato da un bug software noto in cui le versioni interessate di Cisco IOS e Cisco IOS XE possono sempre impostare la data di scadenza del certificato autofirmato su 01/01/2020 00:00:00 UTC. Dopo questa data, il certificato scade e non è valido, il che potrebbe influire sulla funzionalità del prodotto.

D: Perché è stata scelta una data di scadenza 1 gennaio 2020 00:00:00 UTC?

I certificati in genere hanno una data di scadenza. Nel caso di questo bug software, la data 1 gennaio 2020 è stata utilizzata durante lo sviluppo di software Cisco IOS e Cisco IOS XE più di 10 anni fa ed è un errore umano.

D: Quali prodotti sono interessati da questo problema?

Tutti i prodotti Cisco con Cisco IOS versioni precedenti a 15.6(03)M07, 15.7(03)M05, 15.8(03)M03 e 15.9(03)M e tutti i prodotti Cisco con Cisco IOS XE versioni precedenti a 16.9.1

D: Cosa devono fare gli utenti?

È necessario esaminare la notifica sul campo per valutare se il problema si è verificato e, in caso affermativo, seguire le istruzioni per la soluzione/soluzione per risolvere il problema.

D: Si tratta di un problema di sicurezza?

No. Non si tratta di una vulnerabilità della sicurezza e non vi è alcun rischio per l'integrità del prodotto.

D: Il protocollo SSH è interessato?

No. SSH utilizza le coppie di chiavi RSA, ma non i certificati, ad eccezione di una configurazione rara. Affinché Cisco IOS possa utilizzare i certificati, deve essere presente la configurazione successiva.

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

D: Quali versioni fisse sono disponibili per le piattaforme Classic Catalyst 2K, 3K, 4K, 6K?

Per le piattaforme Polaris (serie 3650/3850/Catalyst 9K), la correzione è disponibile a partire dalla versione 16.9.1
Per la piattaforma CDB, la correzione è disponibile a partire dalla versione 15.2(7)E1a

Per le altre piattaforme di switching classiche:

I commit sono in corso, ma non è stato inviato il rilascio CCO. La prossima release CCO può avere la correzione.

Nel frattempo, utilizzare una delle altre soluzioni disponibili.

D: Il problema è WAAS?

WAAS continua a funzionare correttamente e a ottimizzare il traffico, tuttavia AppNav-XE e Central Manager sono stati disconnessi dal dispositivo con un certificato autofirmato scaduto. Ciò significa che non è possibile monitorare AppNav-Cluster o modificare i criteri per WAAS. In breve, WAAS continua a funzionare correttamente, ma la gestione e il monitoraggio vengono sospesi fino alla risoluzione del problema. Per risolvere il problema, può essere necessario generare un nuovo certificato in Cisco IOS e quindi importarlo in Central Manager.

Informazioni correlate

- Vedere FN70489 Notifica: FN - 70489 - Scadenza certificato autofirmato PKI in Cisco IOS e software Cisco IOS XE
- Vedere l'ID bug Cisco CSCvi48253

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).