Procedura per il rinnovo di un certificato autofirmato scaduto in Cyber Vision Center

Sommario

Introduzione

Questo documento descrive la procedura necessaria per rinnovare un certificato autofirmato (SSC) scaduto su un Cisco Cyber Vision Center.

Problema

I certificati utilizzati dal centro per la comunicazione con i sensori per l'interfaccia Web (se non esiste un certificato esterno) vengono generati al primo avvio del centro e sono validi per **2 anni** (con un periodo di tolleranza aggiuntivo di 2 mesi). Una volta raggiunto il tempo, i sensori non saranno più in grado di connettersi al centro, mostrando il seguente tipo di errori nei registri:

```
2023-08-04T09:47:53+00:00 c4819831-bf01-4b3c-b127-fb498e50778d sensorsyncd[1]: 04/08/2023 09:47:53 sensc
```

Inoltre, la connessione all'interfaccia utente Web visualizzerà un errore o verrà bloccata a seconda del browser Web se non è in uso alcun certificato esterno.

Soluzione

È applicabile alla versione 4.2.x. Per le versioni 4.2.1 e successive, può essere eseguito anche dalla GUI Web.

Passaggi per la rigenerazione del certificato del centro

1. Convalida il certificato corrente

```
root@center:~# openssl x509 -subject -startdate -enddate -noout -in /data/etc/ca/center-cert.pem
subject=CN = CenterDemo
notBefore=Aug 8 11:42:30 2022 GMT
notAfter=Oct 6 11:42:30 2024 GMT
```

2. Genera un nuovo certificato
Per generare il nuovo certificato, è necessario utilizzare il nome comune (dal campo "subject=CN") ottenuto

dalla fase precedente

```
root@center:~# sbs-pki --newcenter=CenterDemo
6C89E224EBC77EF6635966B2F47E140C
```

3. Riavviare il Centro.

Per quanto riguarda le installazioni sia con il Centro locale che con il Centro globale, è essenziale annullare la registrazione dei Centri locali e iscriverli nuovamente.

Procedura per la rigenerazione del certificato del sensore

Se il certificato del centro è scaduto, è possibile che alcuni certificati dei sensori stiano per scadere, in quanto sono validi anche 2 anni dal momento in cui il sensore viene creato al centro.

- Per i sensori installati con l'estensione, la ridistribuzione utilizzerà un nuovo certificato.
- Per i sensori installati manualmente:

1. Generare un nuovo certificato al centro con il numero di serie del sensore:

```
root@center:~# sbs-pki --newsensor=FCWTEST
326E50A526B23774CBE2507D77E28379
```

Notare l'ID restituito dal comando

2. Ottieni l'ID sensore per questo sensore

```
root@center:~# sbs-sensor list
c6e38190-f952-445a-99c0-838f7b4bbee6
    FCWTEST (serial number=FCWTEST)
    version:
    status: ENROLLED
    mac:
    ip:
    capture mode: optimal
    model: IOX
    hardware:
    first seen on 2022-08-09 07:23:15.01585+00
    uptime 0
    last update on: 0001-01-01 00:00:00+00â€‹
```

3. Aggiorna il database per il sensore con l'ID certificato

```
root@center:~# sbs-db exec "UPDATE sensor SET certificate_serial='326E50A526B23774CBE2507D77E28379' WHEF
UPDATE 1
```

Il numero di serie del certificato deve essere il valore ottenuto dal primo passaggio e deve essere l'ID sensore del sensore

4. Scaricare il pacchetto di provisioning per questo sensore dalla GUI Web

5. Ripetere la distribuzione con questo pacchetto di provisioning

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).