Steps to renew an expired self-signed certificate in Cyber Vision Center

Contents

Introduction

This document describes the steps involved to renew an expired Self-Signed Certificate (SSC) on a Cisco Cyber Vision Center.

Problem

Certificates used by the center for communication with the sensors for the web interface (if there is no external certificate) are generated on the first startup of the center and are valid for **2 years** (with an additional 2 months grace period). Once the time is reached, the sensors will not be able to connect to the center anymore, showing the following kind of errors in the logs:

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

Additionally, connecting to the web UI will display an error or be blocked depending on the web browser if there is no external certificate in use.

Solution

It's applicable for version 4.2.x. For versions 4.2.1 & greater, it can be done from the Web GUI as well.

Steps to regenerate the Center Certificate

1. Validate the current certificate

```
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. Generate a new certificate
You must use the Common Name (from the "subject=CN" field) obtained from the previous step to generate the new certificate

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

3. Reboot the Center.

On deployments with both Local Center and Global Center, itâ€™s essential to unregister the Local Centers and re-enroll them.

Steps to regenerate the Sensor Certificate

If the center certificate has expired, itâ€™s possible that some sensor certificates are about to expire as those are also valid 2 years from the moment the sensor is created in the center.

- For sensors installed with the extension, redeploying will use a new certificate.
- For sensors that were manually deployed:

1. Generate a new certificate on the center with the sensor serial number:

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

Note the id returned by the command

2. Get the sensor id for this sensor

```
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. Update the database for the sensor with the certificate id

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

Certificate serial must be the value obtained from the first step and id the sensor id of the sensor

4. Download the provisioning package for this sensor from the Web GUI

5. Redo the deployment with this provisioning package