Secure Endpoint Private Cloud - Authentication Certificates Expiration

Contents

Introduction

This document describes the required information around the expiration of authentication certificates in **Cisco Secure Endpoint Private Cloud running versions 3.1.0 to 4.1.0 with an original install of 4 years ago (2020).**

Note: The expiration of these certificates will vary based on when your appliance was setup.

Technical Details

Affected Versions: Cisco Secure Endpoint Private Cloud running versions 3.1.0 to 4.1.0 with an original install of 4 years ago.

Beginning in May 2024, authentication certificates on Secure Endpoint Private Cloud running versions 3.1.0 to 4.1.0 with an original install of 4 years ago will expire. This will cause a service interruption. You will receieve the following warnings in the Administration Console prior to the certificates expiration:

```
System Warning 2024-02-12 00:05:07 +0000 Certificate audit.crt will expire in 3 months.

System Warning 2024-02-12 00:05:07 +0000 Certificate refresh_token.crt will expire in 3 months.

System Warning 2024-02-12 00:05:07 +0000 Certificate jwt.crt will expire in 3 months.

System Warning 2024-02-12 00:05:06 +0000 Certificate saml.crt will expire in 3 months.
```

You can check the expiration date of these certificates using a command line command over SSH as shown below:

```
[root@fireamp certs]# /usr/bin/openssl x509 -text -noout -in /opt/fire/etc/ssl/certs/refresh_token.crt

Certificate:

    Data:

        Version: 3 (0x2)

        Serial Number:

            ee:ea:9f:f9:88:09:38:31:0b:90:bb:b5:1b:29:e3:6b

    Signature Algorithm: sha256WithRSAEncryption

        Issuer: C=US, O=Sourcefire, O=Immunet, OU=PrivateCloud Appliance, CN=refresh-token

        Validity

            Not Before: Sep 28 00:52:02 2022 GMT

            Not After : Sep 27 00:52:02 2026 GMT

        Subject: C=US, O=Sourcefire, O=Immunet, OU=PrivateCloud Appliance, CN=refresh-token
```

When updating to Secure Endpoint Private Cloud 4.2.0, the following certificates will be renewed:

- audit.crt- Signatures for audit records
- refresh_token.crt- Handles communication with identity management service
- jwt.crt- Allows cross-communication between services
- saml.crt- Signs SAML Responses

Impact

If the certificates are not updated before they expire, access to the Administration Console and the Secure Endpoint Console will be lost. Therefore, it is critical that the appliance is updated before the certificates expire in May 2024.

Solution

To update the certificates, the Private Cloud appliance must be updated to at least version 4.2.0. An update can be initiated from the command line over SSH or from the Administration Console user interface.

Tip: Before you begin, please be sure to read the Secure Endpoint Private Cloud Release Notes and Administration Portal User Guide linked at the bottom of this document.

Caution: Prior to updating the appliance to 4.2.0, the content needs to be updated to a recent, after-February 2024 version. Please refer to the Release Notes linked in this document.

From the Administrative Portal:

1. Navigate to **Operations > Update Device**
2. Select **Check/Download Updates**
3. After the update is downloaded, select **Update Software** and choose **OK** to confirm.

From the Command Line via SSH:

1. Run the command **amp-ctl update-check.**
2. After the update is downloaded, run the command **amp-ctl update**.

You can verify the certificates were successfully updated by following the instructions listed in the Technical Details section of this document.

Note: If the appliance cannot be updated due to an urgent situation, please reach out to Cisco TAC here.

Secure Endpoint Private Cloud Release Notes: https://docs.amp.cisco.com/Private%20Cloud%20Release%20Notes.pdf

Secure Endpoint Private Cloud Administration Portal User Guide: https://docs.amp.cisco.com/AMPPrivateCloudAdminGuide-latest.pdf