Restaure la conectividad de telemetría inactiva debido a fallas de renovación de certificados PKI en dispositivos IOS-XE administrados por Catalyst Center que ejecutan las versiones 17.12.1 a 17.12.4.

Introducción

Este documento describe las razones por las que fallan las conexiones de telemetría y cómo restaurarlas.

- La renovación automática del certificado sdn-network-infra-iwancertificate (Cisco Catalyst Center - dispositivo Cisco IOS® XE) puede fallar en un dispositivo Cisco IOS XE debido al ID de bug de Cisco CSCwk39268 en ese sistema operativo del dispositivo Cisco IOS XE, haciendo que la telemetría enviada desde los dispositivos afectados a Catalyst Center se desactive.
- El certificado tiene una validez de un año y normalmente Catalyst Center lo renueva automáticamente unos 60 días antes de que caduque.
- Los clientes afectados por este problema, o que es probable que se vean afectados, pueden ver un mensaje emergente en Catalyst Center.

Versiones afectadas:

- Catalyst Center versiones anteriores a la 2.3.7.11 administración de los dispositivos de red Cisco IOS XE que ejecutan las versiones 17.12.1-17.12.4

Resolución:

Los clientes deben utilizar cualquiera de estas tres opciones para resolver el problema.

Opción 1: Actualice Catalyst Center a 2.3.7.11 o 2.3.7.9 PSMU60 o 2.3.7.10 PSMU110. SMU (Software Maintenance Update) estará disponible para su actualización en System > Software

Management en la GUI de Cisco Catalyst Center.

Opción 2: Actualizar el dispositivo Cisco IOS XE afectado a 17.12.5 o posterior de una versión recomendada por Cisco.

Opción 3: Fuerce la telemetría de inserción desde la GUI de Catalyst Center y actualice el algoritmo hash para el trustpoint a sha512 en el dispositivo de la siguiente manera:

1. Vaya a Menú > Aprovisionar > Inventario.
2. Seleccione los dispositivos por nombre de host
3. Seleccione Actions > Telemetry > Update Telemetry Settings
4. Habilitar transferencia de configuración forzada
5. Vaya al asistente y envíe la tarea

Identificación del dispositivo Cisco IOS XE afectado:

Paso 1: Validar el certificado del dispositivo y el estado del punto de confianza en el dispositivo Cisco IOS XE afectado.

```
device# show crypto pki certificates verbose sdn-network-infra-iwan
```

Ejemplo de Salida:

```
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 18831279321B12FA
  Certificate Usage: General Purpose
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    Name: device.example.net
    cn=C9300-48U_SN12345678_sdn-network-infra-iwan
    hostname=device.example.net
  Validity Date:
    start date: 11:39:55 cdt Jul 10 2025
    end   date: 11:39:55 cdt Jul 16 2025
    renew date: 06:51:54 cdt Jul 15 2025
  ...
```

Nota: Si la fecha de finalización y la fecha de renovación son anteriores a la fecha actual en el

dispositivo, el certificado ha caducado.

Paso 2: Compruebe el registro de errores en el dispositivo.

Ejemplo de Salida:

```
Device# show logging
%PKI-2-CERT_RENEW_FAIL: Certificate renewal failed for trustpoint sdn-network-infra-iwan
Reason : Failed to get ID certificate from CA server sdn-network-infra-iwan:Certificate renewal failed.
```

Paso 3: Compruebe el estado de telemetría del dispositivo en el centro de Catalyst

Ejemplo de Salida:

```
Device#show tel con all
Telemetry connections
Index Peer Address Port VRF Source Address State State Description
--------------------------------------------------------------------------------
36284 x.x.x.x 25103 0 x.x.x.x Connecting Connection request made to transport handler
```

Nota: En este ejemplo, la conexión de telemetría no está activa, solo en el estado Conexión.

Información adicional:

(a.) En el caso de varios dispositivos Cisco IOS XE, esta plantilla puede extraerse de Catalyst Center mediante el aprovisionamiento de plantillas CLI desde las herramientas Diseño > Plantillas CLI:

```
crypto pki trustpoint sdn-network-infra-iwan
no hash sha256
hash sha512
```

(b) Forzar inserción de telemetría tras actualización de hash

1. Vaya a Menú > Aprovisionar > Inventario.
2. Seleccione los dispositivos por nombre de host
3. Seleccione Actions > Telemetry > Update Telemetry Settings
4. Habilitar transferencia de configuración forzada
5. Vaya al asistente y envíe la tarea

Preguntas frecuentes: ¿La instalación de SMU corrige un sistema ya afectado o es preventiva? SMU es una solución preventiva y debe instalarse antes de que se produzca el problema. Si el problema ya ha ocurrido, la instalación de SMU no lo borrará automáticamente. Para recuperar los sistemas con fallos existentes, seleccione la opción 3.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).