Error de validación de certificado de acceso seguro con cargas de registro de clientes Splunk

Contenido

Problema

Los clientes de Windows que ejecutan el cliente Splunk no pudieron cargar registros en la nube Splunk debido a errores de validación de certificados cuando Cisco Secure Access descifró el tráfico. Más de 5000 orígenes de registro de Windows no pudieron enviar datos a la nube de Splunk, lo que afectó a la ingestión de registro. El error específico observado en los registros del cliente Splunk fue:

```
02-27-2026 16:51:54.830 +0530 ERROR X509Verify [15668 TcpOutEloop] - Server X509 certificate failed val
```

El tráfico al destino *.splunkcloud.com fluía a través del firewall, pero la validación del certificado de nivel de aplicación fallaba. La navegación web a sitios en los que se ha habilitado el descifrado SSL ha seguido funcionando normalmente.

Entorno

- Cisco Secure Access con descifrado SSL/TLS habilitado
- Clientes de Windows con Splunk Universal Forwarder instalado
- Destino de la nube Splunk: *.splunkcloud.com
- Más de 5000 orígenes de registro de Windows afectados
- El cliente Splunk utiliza su propio almacén de certificados, no el almacén de certificados del sistema de Microsoft

Resolución

El problema se resolvió implementando una política de omisión del descifrado para el tráfico en la nube Splunk en Cisco Secure Access.

Se adoptaron varias medidas.

Paso 1: ‘Identificar el problema’

Durante una sesión de WebEx, se confirmó y reprodujo el comportamiento. Las pruebas mostraron que cuando el descifrado de Secure Access estaba desactivado para un cliente o cuando el servicio SWG estaba desactivado en el cliente, las cargas de registro de Splunk se realizaban correctamente. Esto confirmó que el proceso de descifrado SSL/TLS estaba causando la falla de validación del certificado.

Paso 2: Crear lista de destino

Se creó una lista de destinos que contiene los FQDN y las direcciones IP de la nube Splunk para dirigir específicamente el tráfico destinado a los servicios de la nube Splunk.

Paso 3: Implementar política de omisión de descifrado

Se implementó una política de Cisco Secure Access para deshabilitar el descifrado SSL/TLS para el tráfico que coincide con la lista de destinos de la nube Splunk. Esta política de omisión permitió a los clientes Splunk establecer conexiones cifradas directas a la nube Splunk sin la intercepción de certificados por Secure Access.

Paso 4: Validación

Después de implementar la política de omisión del descifrado, la validación confirmó que:

- Los clientes Splunk pudieron cargar los registros correctamente
- El número total de clientes de informes en la nube Splunk aumentó considerablemente
- No se observaron más errores de validación de certificados

La gravedad de los casos se redujo de 1 a 3 y se pasó al estado de supervisión para observar una correcta ingestión continua de registros.

Causa

La causa raíz fue que el cliente Splunk utiliza su propio almacén de certificados y no confía en el certificado de la subCA principal de Cisco Secure Access que se presentó durante el descifrado SSL/TLS. Cuando Cisco Secure Access interceptó y descifró el tráfico SSL en la nube Splunk, volvió a cifrar el tráfico usando su propia autoridad de certificados. El proceso de validación de certificados del cliente Splunk rechazó este certificado porque no pudo comprobar la cadena de certificados de vuelta a una entidad emisora de certificados raíz de confianza en su propio almacén de certificados.

El error de validación X.509 específico "no se puede obtener el certificado de emisor local" (código de error 20) indica que el proceso de validación de certificados no pudo encontrar la entidad emisora de certificados en el almacén de certificados de confianza del cliente, lo que provocó un error en la conexión.

Contenido relacionado

- Soporte técnico y descargas de Cisco

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).