Solución de problemas de error de vencimiento de certificado durante Umbrella Integration Access

Contenido

Introducción

Problema

Causa

Resolución

Introducción

Este documento describe cómo resolver un error de vencimiento de certificado cuando una integración de Umbrella accede a s-platform.api.opendns.com o a fireeye.vendor.api.opendns.com.

Problema

Las integraciones de Umbrella que utilizan algunos clientes de terceros pueden fallar con un error al verificar el certificado digital del servidor para las API de Umbrella en s-platform.api.opendns.com and fireeye.vendor.api.opendns.com. El texto o código de error varía según el programa cliente utilizado en la integración, pero normalmente indica que hay un certificado caducado.

Causa

Este problema no se debe al certificado del servidor, que es válido actualmente. Más bien, el problema se debe a un almacén de confianza de certificados obsoleto utilizado por el cliente.

El servidor web que sirve a s-platform.api.opendns.com y fireeye.vendor.api.opendns.com utiliza un certificado digital emitido (que está firmado digitalmente) por el certificado intermedio R3 de la autoridad de certificación Let's Encrypt. R3 está firmado por una clave pública que se encuentra tanto en el Certificado raíz X1 SRG de Let's Encrypt, y una versión antigua de la raíz X1 SRG con firma cruzada. Por lo tanto, existen dos rutas de validación: uno que termina en la raíz SRG actual X1 y otro que termina en el emisor de la versión con firma cruzada, el certificado DST Root CA X3, emitido por la autoridad de certificación IdenTrust.

Un diagrama de la emisión está disponible en Let's Encrypt. Además, la herramienta Qualys SSL Labs se puede utilizar para ver las dos "rutas de certificación" con sus certificados respectivos y los detalles del certificado, como las fechas de vencimiento.

Los certificados raíz se mantienen en uno o más almacenes de confianza de certificados en los sistemas cliente. El 30 de septiembre de 2021 caducó el certificado X3 de CA raíz de DST. Desde esta fecha, los clientes que tienen el certificado X3 de CA raíz DST en su almacén de confianza, pero no tienen el certificado raíz X1 de raíz RG más reciente, no pueden conectarse a s-platform.api.opendns.com o fireeye.vendor.api.opendns.com debido a un error de certificado. El mensaje o código de error puede indicar un certificado caducado como motivo del error. El certificado caducado es el certificado X3 de CA raíz de DST en el almacén de confianza del cliente, no el certificado de servidor para los servidores API, s-platform.api.opendns.com y fireeye.vendor.api.opendns.com.

Resolución

Para solucionar este problema, actualice el almacén de confianza del cliente para incluir el nuevo certificado SRG Root X1, que se puede descargar del sitio web Let's Encrypt. (Esta página también proporciona sitios web para probar sus clientes.) Consulte la documentación del cliente o sistema operativo para obtener instrucciones sobre cómo ver y actualizar el almacén de confianza del cliente. Si hay disponible un paquete de actualización oficial o un mecanismo de actualización automática, normalmente es preferible a actualizar manualmente el almacén de confianza.

Si actualiza manualmente el almacén de confianza con el nuevo certificado X1 de raíz SRG, también recomendamos eliminar el certificado X3 de CA raíz DST caducado, en caso de que el código de creación de rutas de validación del cliente sea problemático. Una actualización oficial del almacén de confianza del proveedor de su cliente o sistema operativo puede agregar la raíz SRG X1 y quitar el certificado DST raíz CA X3.

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).