Solucionar Problemas de Erro de Vencimento de Certificado durante o Acesso de Integração do Umbrella

Contents

Introdução

Este documento descreve como solucionar problemas de um erro de expiração de certificado quando uma integração do Umbrella acessa s-platform.api.opendns.com ou fireeye.vendor.api.opendns.com.

Problema

As integrações do Umbrella que usam alguns clientes de terceiros podem falhar com um erro de verificação do certificado digital do servidor para as APIs do Umbrella em s-platform.api.opendns.com and fireeye.vendor.api.opendns.com. O texto ou código de erro varia dependendo do programa cliente usado na integração, mas geralmente indica que um certificado expirado está presente.

Causa

Esse problema não é causado pelo certificado do servidor, que é válido no momento. Em vez disso, o problema é causado por um armazenamento de confiança de certificado desatualizado usado pelo cliente.

O servidor da Web que serve s-platform.api.opendns.com e fireeye.vendor.api.opendns.com usa um certificado digital que é emitido (que é assinado digitalmente) pelo certificado intermediário R3 da autoridade de certificação Let's Encrypt. R3 é assinado por uma chave pública encontrada nos Certificado raiz SRG Root X1 da Let's Encrypt e uma versão mais antiga da Raiz SRG X1 com assinatura cruzada. Assim, existem dois caminhos de validação: uma que termina na raiz SRG atual X1 e outra que termina no emissor da versão assinada, o certificado DST Root CA X3, emitido pela autoridade de certificação IdenTrust.

Um diagrama da emissão está disponível em Let's Encrypt. Além disso, a ferramenta Qualys SSL Labs pode ser usada para visualizar os dois "caminhos de certificação" com seus respectivos

certificados e os detalhes do certificado, como as datas de expiração.

Os certificados raiz são mantidos em um ou mais armazenamentos de certificados confiáveis em sistemas cliente. Em 30 de setembro de 2021, o certificado raiz do Horário de Verão CA X3 expirou. Desde essa data, os clientes que têm o certificado raiz DST CA X3 em seu armazenamento confiável, mas não têm o certificado raiz RG X1 mais recente, não conseguem se conectar a s-platform.api.opendns.com ou fireeye.vendor.api.opendns.com devido a um erro de certificado. A mensagem de erro ou o código pode indicar um certificado expirado como a razão do erro. O certificado expirado é o certificado da CA X3 raiz do Horário de Verão no repositório de confiança do cliente, não o certificado do servidor para os servidores de API, s-platform.api.opendns.com e fireeye.vendor.api.opendns.com.

Resolução

Para corrigir esse problema, atualize o armazenamento confiável do cliente para incluir o novo certificado SRG Root X1, que pode ser baixado do site Let's Encrypt. (Esta página também fornece sites para testar seus clientes.) Consulte a documentação do cliente ou do sistema operacional para obter instruções sobre como exibir e atualizar a loja confiável do cliente. Se um pacote de atualização oficial ou um mecanismo de atualização automática estiver disponível, isso geralmente é preferível à atualização manual do armazenamento confiável.

Se estiver atualizando manualmente o armazenamento confiável com o novo certificado SRG Root X1, recomendamos também a remoção do certificado expirado da CA X3 da raiz do Horário de Verão, caso o código de criação do caminho de validação do seu cliente seja problemático. Uma atualização oficial do armazenamento confiável do provedor do seu cliente ou sistema operacional pode adicionar o SRG Root X1 e remover o certificado DST Root CA X3.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.