Dépannage des erreurs d'expiration de certificat pendant Umbrella Integration Access

Table des matières

Introduction

Ce document décrit comment dépanner une erreur d'expiration de certificat lorsqu'une intégration Umbrella accède à s-platform.api.opendns.com ou à fireeye.vendor.api.opendns.com.

Problème

Les intégrations Umbrella qui utilisent certains clients tiers peuvent échouer avec une erreur de vérification du certificat numérique du serveur pour les API Umbrella à l'adresse s-platform.api.opendns.com and fireeye.vendor.api.opendns.com. Le texte ou le code d'erreur varie en fonction du programme client utilisé dans l'intégration, mais indique généralement la présence d'un certificat expiré.

Motif

Ce problème n'est pas causé par le certificat du serveur, qui est actuellement valide. Le problème est plutôt causé par un magasin de certificats de confiance obsolète utilisé par le client.

Le serveur Web qui dessert s-platform.api.opendns.com et fireeye.vendor.api.opendns.com utilise un certificat numérique qui est émis (qui est signé numériquement) par le certificat intermédiaire R3 de l'autorité de certification Let's Encrypt. R3 est signé par une clé publique qui se trouve dans la Le certificat racine SRG Root X1 de Let's Encrypt et une version plus ancienne et avec signatures croisées de SRG Root X1. Il existe donc deux chemins de validation : une qui se termine au niveau de la racine X1 SRG actuelle, et une qui se termine au niveau de l'émetteur de la version à signature croisée, le certificat DST Root CA X3, émis par l'autorité de certification IdenTrust.

Un schéma de l'émission est disponible à partir de Let's Encrypt. En outre, l'outil Qualys SSL Labs peut être utilisé pour afficher les deux « chemins de certification » avec leurs certificats respectifs et les détails du certificat, tels que les dates d'expiration.

Les certificats racines sont conservés dans un ou plusieurs magasins de certificats de confiance

sur les systèmes clients. Le 30 septembre 2021, le certificat DST Root CA X3 a expiré. Depuis cette date, les clients qui ont le certificat DST Root CA X3 dans leur magasin de confiance, mais qui n'ont pas le certificat racine RG Root X1 plus récent, ne parviennent pas à se connecter à s-platform.api.opendns.com ou fireeye.vendor.api.opendns.com en raison d'une erreur de certificat. Le message ou le code d'erreur peut indiquer un certificat expiré comme raison de l'erreur. Le certificat expiré est le certificat X3 de l'autorité de certification racine de l'heure d'été dans le magasin de confiance du client, et non le certificat du serveur pour les serveurs d'API, s-platform.api.opendns.com et fireeye.vendor.api.opendns.com.

Résolution

Pour résoudre ce problème, mettez à jour le magasin de confiance du client afin d'inclure le nouveau certificat SRG Root X1, qui peut être téléchargé à partir du site Web Let's Encrypt. (Cette page fournit également des sites Web pour tester vos clients.) Consultez la documentation de votre client ou de votre système d'exploitation pour obtenir des instructions sur l'affichage et la mise à jour du magasin de confiance de votre client. Si un package de mise à jour officiel ou un mécanisme de mise à jour automatique est disponible, il est généralement préférable de mettre à jour manuellement le magasin approuvé.

Si vous mettez à jour manuellement le magasin de confiance avec le nouveau certificat SRG Root X1, nous vous recommandons également de supprimer le certificat DST Root CA X3 expiré, au cas où le code de création de chemin de validation de votre client poserait problème. Une mise à jour officielle du magasin de confiance du fournisseur de votre client ou système d'exploitation peut ajouter le SRG Root X1 et supprimer le certificat DST Root CA X3.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.