Umbrella統合アクセス時の証明書有効期限エラーのトラブルシューティング

内容

はじめに

このドキュメントでは、Umbrella統合がs-platform.api.opendns.comまたはfireeye.vendor.api.opendns.comにアクセスする際に発生する証明書有効期限エラーのトラブルシューティング方法について説明します。

問題

一部のサードパーティ製クライアントを使用するUmbrella統合は、s-platform.api.opendns.com and fireeye.vendor.api.opendns.comで、Umbrella API用のサーバのデジタル証明書の検証エラーにより失敗する可能性があります。エラーテキストまたはコードは、統合で使用されるクライアントプログラムによって異なりますが、通常は期限切れの証明書があることを示します。

原因

この問題は、現在有効なサーバの証明書が原因ではありません。むしろ、クライアントが使用する古い証明書信頼ストアが問題の原因です。

s-platform.api.opendns.comおよびfireeye.vendor.api.opendns.comにサービスを提供するWebサーバは、認証局(CA)のLet's Encryptから中間証明書R3によって発行された（デジタル署名された）デジタル証明書を使用します。R3は公開キーによって署名されており、この公開キーは Let's EncryptからのSRG Root X1ルート証明書、およびSRG Root X1の古い相互署名付きバージョン。したがって、2つの検証パスが存在します。1つは現在のSRGルートX1で終了する検証パスで、もう1つは認証局(CA)Identrustによって発行されたクロス署名バージョンDST Root CA X3証明書の発行者で終了する検証パスです。

この発行の図は、「Let’s Encrypt」から入手できます。また、Qualys SSL Labsツールを使用すると、それぞれの証明書と証明書の詳細（有効期限など）が記載された2つの「認証パス」を表示できます。

ルート証明書は、クライアントシステム上の1つ以上の証明書信頼ストアに保持されます。2021年9月30日に、DSTルートCA X3証明書の期限が切れました。この日付以降、信頼ストアに

DSTルートCA X3証明書があっても、新しいRGルートX1ルート証明書がないクライアントは、証明書エラーが原因でs-platform.api.opendns.comまたはfireeye.vendor.api.opendns.comへの接続に失敗します。 エラーメッセージまたはコードは、エラーの理由として期限切れの証明書を示している可能性があります。期限切れの証明書は、APIサーバ(s-platform.api.opendns.comおよびfireeye.vendor.api.opendns.com)のサーバ証明書ではなく、クライアントの信頼ストアにあるDSTルートCA X3証明書です。

解決方法

この問題を解決するには、クライアントの信頼ストアを更新して、新しいSRGルートX1証明書を追加します。この証明書はLet's Encrypt Webサイトからダウンロードできます。（このページには、クライアントをテストするためのWebサイトもあります）。 クライアントの信頼ストアを表示および更新する手順については、クライアントまたはオペレーティングシステムのマニュアルを参照してください。正式なアップデートパッケージまたは自動更新メカニズムが使用可能な場合、通常は手動で信頼ストアを更新するよりも、この方法が適しています。

新しいSRG Root X1証明書で信頼ストアを手動で更新する場合、クライアントの検証パス構築コードに問題がある場合に備えて、期限切れのDST Root CA X3証明書も削除することをお勧めします。クライアントまたはオペレーティングシステムのプロバイダーからの信頼ストアの公式アップデートでは、SRG Root X1を追加し、DST Root CA X3証明書を削除できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。