FirefoxおよびSafari(macOS)でのセキュアアクセスのカスタムCAの信頼に関する問題

内容

問題

Cisco Secure Accessを介して復号化されたインターネットトラフィックにアクセスすると、macOSブラウザ（SafariおよびFirefox）で証明書信頼エラーが発生します。Chromeブラウザは正常に動作しましたが、SafariとFirefoxでは「信頼できない証明書」警告が表示され、Webサイトやアプリケーションへのアクセスがブロックされました。

完全な証明書チェーンは次のようになります。

- Webサイト（cnn.comなど） > Cisco Secure Access Custom CA > Cisco Secure Access Custom R3 CA > Cisco Secure Access Custom CA > xxxx-SUBCA1 > xxxxROOT-CA

FirefoxおよびSafariブラウザでは、シスコ中間証明書での証明書の検証が停止し、ルートCAへのチェーン接続に失敗しましたが、Chromeでは証明書チェーン全体が正常に検証されました。

環境

- HTTPS復号用のカスタム認証局を使用したCisco Secure Accessの導入
- safariおよびFirefoxブラウザ対応のmacOSデバイス
- Microsoft認証局を使用したカスタムCA証明書インフラストラクチャ
- 復号化と侵入防御が有効なインターネットアクセスポリシー
- 組織ID:xxxxx

解決方法

この問題は、証明書チェーンのエンコードの不一致を特定し、復号のためにCisco Secure AccessルートCAに切り替えることで解決されました。

根本原因の分析

チームは、印刷可能な文字列エンコードを使用してカスタム証明機関が作成されたことを特定しました。これにより、リーフ証明書がUTF8STRINGに設定されている場合でも互換性の問題が発生しました。FirefoxとSafariでは、チェーン内のすべての証明書が同じ形式であることが必要ですが、Chromeではこの厳格な要件はありません。

解決手順

Cisco Secure AccessルートCAへの切り替え

代替ソリューション

カスタムCAを使用する必要がある場合は、次のオプションが指定されています。

- UTF8エンコーディングを使用して証明書インフラストラクチャ全体を再構築する（影響が大きい、推奨されない）
- UTF8エンコードをサポートする別の証明書インフラストラクチャを使用する
- FirefoxおよびSafariの制限は、現在のカスタムCA設定では機能しません

原因

根本原因は、Microsoft認証局（デフォルトでprintablestringエンコーディングを使用）とCisco Secure Accessで使用されるUTF8チェーンの間のエンコーディングの不一致でした。FirefoxとSafariでは証明書の検証がより厳しく、チェーン内のすべての証明書で一貫したエンコーディングを使用する必要があります。Chromeでの検証がより緩やかになったため、混合エンコーディングチェーンで機能し、FirefoxとSafariでは一貫性のない証明書フォーマットが拒否されました。

Microsoft CAはprintablestringエンコーディングを使用して証明書を作成しましたが、Cisco Secure Access中間証明書はUTF8STRINGエンコーディングを使用しました。この不一致が原因で、FirefoxおよびSafariではシスコの中間証明書レベルでの証明書チェーン検証が失敗します。

関連コンテンツ

- SWGでのWebex Meeting Accessの設定
- シスコのテクニカルサポートとダウンロード

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。