一般的な証明書およびTLSプロトコルエラーについて

内容

はじめに

このドキュメントでは、Umbrellaダッシュボードのアクティビティ検索で発生する一般的な証明書およびTLSプロトコルエラーについて説明します。

概要

証明書およびTLSエラーが原因でブロックされたHTTPトラフィックを、Umbrellaダッシュボードのアクティビティ検索で表示できるようになりました。この記事では、一般的なエラーメッセージのリストと、各エラーの簡単な説明を示します。

証明書エラー

アップストリーム証明書の期限切れ

Webサイトで提示された証明書の有効期限が切れています。この問題を報告するには、サイトのWebマスターに問い合わせてください。

アップストリーム証明書の自己署名

Webサイトによって提示されたサーバー証明書は証明機関によって署名されていないため、Umbrellaは証明書が信頼できるかどうかを判断できません。

自己署名証明書は、制限された対象者向けのリソースをサーバがホストする場合に使用されることがあります。たとえば、I.T.セキュリティアプライアンスのWebポータルでは、多くの場合、自己署名証明書がデフォルトで使用されます。自己署名証明書を信頼するようにUmbrellaを構成することはできません。

中間証明書がありません

Umbrellaは、すべての中間機関の証明書を取得できなかったため、信頼のチェーン全体を検証できませんでした。

Webサーバ証明書は通常、認証局(CA)の中間証明書として発行/署名されます。これらの中間証明書は、他の中間証明書によって発行することもできます。Webサーバ証明書 (別名「リーフ証明書」) と中間証明書は、ルート証明書へのチェーンを形成します。Umbrellaが完全な信頼のチェーンを検証するには、Webサイトで中間証明書とサーバ証明書をバンドルする必要があります。この問題を報告するには、サイトのWebマスターに問い合わせてください。

または、証明書に「Authority Information Access」拡張子が含まれている場合、Umbrellaは中間CAを自動的に取得しようとします。HTTPS復号化とファイルインスペクションが有効になっている場合、UmbrellaはAIA拡張子のみをサポートすることに注意してください。

アップストリーム証明書にサブジェクト名がありません。

証明書のサブジェクトフィールドには、この証明書を識別するための識別名(DN)が含まれていません。これは、認証局によって発行されるすべての証明書の要件であるため、Cisco Umbrellaに必要です。この問題を報告するには、サイトのWebマスターに問い合わせてください。

アップストリーム証明書に共通名がありません。

Webサイトで提示される証明書に共通名がありません。Umbrella SWGでは、Common Name(CN)フィールドが必要です。これには、証明書のホスト名が含まれます。これは、証明書がユーザによって要求されたリソース(例：ブラウザに入力したアドレス)。 この問題を報告するには、サイトのWebマスターに問い合わせてください。

アップストリーム証明書の信頼なし

証明書がCisco Umbrellaで信頼されていないこのエラーは通常、証明書を発行したルートCAをCiscoが信頼していないことを意味します。

Umbrella SWGには、信頼できる既知のルート認証局のリストが組み込まれており、信頼できるソースから更新します。Webサイトの証明書がこのリストのCAによって署名されていない場合、証明書の検証は失敗します。Umbrellaに信頼できるルートCAがないと思われる場合は、テクニカルサポートにお問い合わせください。

証明書のホスト名が予期されたものと異なります

ユーザが要求したリソース（ブラウザに入力したアドレスなど）が、証明書の共通名(CN)またはサブジェクト代替名(SAN)と一致しません。そのため、Umbrellaはこの要求の証明書を信頼できません。この問題を報告するには、サイトのWebマスターに問い合わせてください。

アップストリーム証明書の失効

Webサイトから提供された証明書が、発行側の認証局によって無効にされています。

Umbrellaは、OCSP(Online Certificate Status Protocol)チェックを実行して、後で証明書がCAによって失効されたかどうかを確認します。この問題を報告するには、サイトのWebマスターに問い合わせてください。

TLSハンドシェイクエラー

サポートされていないアップストリーム暗号

TLSハンドシェイクを完了できませんでした。これは通常、WebサイトがUmbrella SWGで使用される暗号スイートのリストをサポートしていないことを意味します。このエラーは、脆弱なTLS暗号しかサポートしていない古いWebサーバで発生する可能性があります。この問題を報告するには、サイトのWebマスターに問い合わせてください。

アップストリームTLSバージョンの不一致

WebサイトがUmbrella SWGが使用するのと同じTLSバージョンをサポートしていないため、TLSハンドシェイクを完了できませんでした。現時点では、Umbrella SWGプロキシは、Umbrella SWGへのクライアント側接続と、宛先WebサーバへのUmbrella SWGプロキシ接続の両方でTLS 1.2とTLS 1.3をサポートしています。

アップストリームDHキーが1024ビット未満

WebサイトでUmbrellaでサポートされていない弱いDiffie-Hellmanキーが使用されているため、TLSハンドシェイクを完了できませんでした。この問題を報告するには、サイトのWebマスターに問い合わせてください。

回避策

Cisco Umbrellaの設定を変更することで、これらの問題を回避できます。この操作は、サーバーと証明書の信頼性が信頼できる場合にのみ実行する必要があります。

「選択的復号化リスト」エントリを使用して復号化を無効にする回避策と、「外部ドメイン」エントリを使用してUmbrellaからのトラフィックを完全にバイパスする回避策があります。復号が無効な場合、Umbrellaは証明書の検証を実行しません。ほとんどの場合、Umbrellaからトラフィックがバイパスされるときにブラウザが引き続きエラーまたは警告を表示することに注意してください。Webブラウザは同様の証明書検証を実行します。

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。