目次

質問

1. Cisco Web セキュリティ アプライアンス（WSA）ストリップ CRL 情報はなぜ HTTPS トラフィックを復号化している間生成された認証からのか。
2. サーバ証明を「生成が SSL 復号化の間にスプーフィングした」ときに、WSA はオリジナル認証から証明書無効リスト（CRL）を除去します。 これはなぜされますか。

環境

WSA バージョン、HTTPS プロキシおよび有効に なる SSL 復号化。

症状

オリジナルサーバ 認証の CRL 情報は WSA の復号化 HTTPS トラフィック、およびこうしてクライアントは認証は取り消されたかどうか確認できないが生成された認証にもはやありません。

WSA は生成された認証のためにもはや有効ではないので CRL 情報を除去します。 説明は CRL がどのようにのはたらくか知識を含みます。

認証局（CA）はオプションでもはや有効と見なさない証明書無効リスト、か CRL と呼ばれる認証のリストを保持できます。 認証はさまざまな理由で取り消されるかもしれません- CA は認証を要求したエンティティがそれらあっただれが言ったかではないか、またはプライベートキーは認証と盗まれて報告されることがある関連付けたことを判別するかもしれません。 署名されたサーバ証明に基づいて Webサーバ識別を検証しているクライアントは認証が取り消されなかったことを確認するために CRL を参照するかもしれません。

CRL は特定の CA によって取り消され、そのリストがシリアル番号によって CA.によって取り消される認証によって識別される署名する認証のリストが含まれています。 クライアントはこの CRL を取得し、次にサーバ証明が CRL にリストされていないことを確認できます。 CRL をダウンロードするための URL は通常認証にフィールドとして含まれています。 実用的な方法として、ほとんどのクライアントは CRL に対して認証を検証しません。

WSA は HTTPS または SSL トラフィックを復号化しているとき、新しいサーバ証明を生成することおよび自身の内部 CA（**HTTPS プロキシ セクションの下でアップロードされるか、または生成される認証**）と署名することによってこれをします。

WSA が CRL 情報を**除去しなかった場合**、CRL を検証したいと思ったクライアントは**認証**および**CRL が異なる認証機関によって署名される**ことが、および CRL を無視するか、または工ラーに

フラグを付けるために分ります。 なお、ある状況下では、WSA はオリジナル認証のシリアル番号と異なるために生成された認証のシリアル番号を変更します。 これはクライアントが CRL と WSA 生成された認証間の CA の違いを無視しても、シリアル番号 情報は有効ではないことを意味します。

問題に対処する最もよい方法はクライアントの為の CRL 自体を、検証し、次に認証から CRL 情報を除く WSA のためです。 WSA はこれを今日することができません。

AsyncOS バージョン 7.7 および それ 以上:

AsyncOS バージョン 7.7 から開始して、CRL へ代替である WSA はオンライン認証ステータスプロトコル（**OCSP**）をサポートします。

有効に されたとき、OCSP は X.509 デジタル認証の取り消し の ステータスを得る機能を提供します。