WSA による HTTPS トラフィックの復号化時に生成された証明書から CRL 情報が除去されるのはなぜですか。

目次

質問

1. HTTPS トラフィックの復号化中に、Cisco Web セキュリティ アプライアンス（WSA）が、生成された証明書から CRL 情報を削除するのはなぜですか?
2. SSL 復号化期間に「偽装」サーバ証明書を生成するときに、WSA は元の証明書から証明書失効リスト（CRL）を削除します。 こうする理由は何ですか?

環境

WSA の任意のバージョン、HTTPS プロキシ、および SSL 復号化が有効になっている。

症状

WSA 上の HTTPS トラフィックの復号化中に生成された証明書から元のサーバ証明書内の CRL 情報が削除されるため、クライアントは証明書が失効したかどうかを確認できません。

WSA は、生成された証明書に対して有効でなくなった CRL 情報を削除します。 説明する前に、まず CRL の機能を理解する必要があります。

認証局（CA）は、有効でなくなったと判断した、証明書失効リスト（CRL）と呼ばれる証明書のリストを任意で維持できます。 証明書はさまざまな理由で失効する可能性があります。CA が、証明書を要求したエンティティが送信元ではないと判断した場合や証明書に関連付けられた秘密キーが盗難に遭ったと報告された場合です。 署名付きサーバ証明書に基づいて Web サーバの ID を検証するクライアントは、CRL を参照して証明書が失効していないことを確認します。

CRL には特定の CA によって失効した証明書のリストが含まれており、そのリストが CA によって署名されます。失効した証明書はシリアル番号で識別されます。 クライアントは、この CRL を取得して、サーバ証明書が CRL に掲載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、証明書内の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 に照らして証明書を検証しません。

WSA は HTTPS または SSL トラフィックを復号化するときに、新しいサーバ証明書を生成し、独自の内部 CA (**HTTPS プロキシ セクションでアップロードまたは生成された証明書**) を使って署名することによってこの処理を行います。

WSA が CRL 情報を削除しなかった場合は、CRL を検証したかっ>たクライアントが**証明書**と **CRL** が**別々の認証局によって署名されている**と判断し、CRL を無視するか、エラーを警告します。 さらに、状況によっては、WSA が生成された証明書のシリアル番号を元の証明書内のシリアル番号から変更する場合もあります。 これは、クライアントが CRL と WSA 生成証明書間の CA の違いを無視したとしても、シリアル番号情報が有効でなくなることを意味します。

この問題を解決する最善の方法は、WSA がクライアントの代わりに CRL 自体を検証し、証明書から CRL 情報を除外することです。 現在、WSA はこの処理を行うことができません。

AsyncOS バージョン 7.7 以降：

AsyncOS バージョン 7.7 以降では、WSA が CRL の代替手段である Online Certification Status Protocol（**OCSP**）をサポートします。

有効になっている場合、OCSP は X.509 デジタル証明書の失効ステータスを取得する機能を提供します。