SGC 接続障害： ステップアップ暗号とエクスポート暗号で異なるダイジェストが使用される

目次

概要

このドキュメントでは、Microsoft Internet Information Server (IIS) および Microsoft Internet Explorer で使用される、セキュリティ プロバイダーの Schannel.dll ファイルで発生する問題について説明します。 この問題は、高度な暗号化を行うために Server Gated Cryptography (SGC) を使用するサイトに接続し、エクスポートの暗号スイートが 1 つのハッシュ アルゴリズムを使用し、その一方で内部の暗号スイートが別のハッシュ アルゴリズムを使用する場合に表示されます。 この場合、Schannel.dll ファイルが誤ったアルゴリズムを選択することがあり、接続の失敗につながります。 その結果、安全な接続が必要な場合に、Web クライアントは強力な暗号化のために SGC を使用する Web サイトに接続できない場合があります。 インターネット サーバまたは Web クライアントで Microsoft 製品を実行している場合は、接続が失敗する可能性があります。

Microsoft 社では、ステップアップ暗号がエクスポート暗号と異なるダイジェストを使用する場合は、接続が失敗することを認識しています。 この問題の詳細については、「ドメスティック クライアントからの SGC 接続が失敗することがある」を参照してください 。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- セキュア ソケット レイヤ（SSL）モジュールを搭載した Cisco Content Services（CSS）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

問題

CSS SSL モジュールに SGC ステップアップ証明書があり、クライアントが 56 ビットのブラウザで SSL モジュールを介してサイトに接続すると、ブラウザは 128 への接続のステップ アップではなく、56 で SSL 接続を確立します。

たとえば、最初のクライアントの hello が暗号 rsa-export1024-with-rc4-56-sha をネゴシエートしているとします。 モジュールは設定の順序に基づいて（暗号が重み付けされていない場合）照合を行います。そのため、ステップアップが発生すると、モジュールはおそらく、rsa-with-3des-ede-cbc-sha を使用しようとします。 これら 2 つの暗号のダイジェストは一致せず、障害が発生します。 ダイジェストは一致する必要があり、さらに、暗号タイプも一致する必要があります。

解決策

顧客のプロキシ リストの例に基づいて、この問題のソリューションをこのセクションで説明します。

現在、顧客には次のエクスポート暗号があります。

- ssl-server 4
- ssl-server 4 vip address 198.22.10.10
- ssl-server 4 rsakey CSSRsaKey4
- ssl-server 4 rsacert RsaCert4
- ssl-server 4 cipher rsa-with-rc4-128-md5 198.22.10.10 20094
- ssl-server 4 cipher rsa-with-rc4-128-sha 198.22.10.10 20094
- ssl-server 4 cipher rsa-with-des-cbc-sha 198.22.10.10 20094
- ssl-server 4 cipher rsa-with-3des-ede-cbc-sha 198.22.10.10 20094
- ssl-server 4 cipher rsa-export1024-with-des-cbc-sha 198.22.10.10 20094
- ssl-server 4 cipher rsa-export1024-with-rc4-56-sha 198.22.10.10 20094

このドキュメントで説明する問題を解決するには、サポートするエクスポート暗号を 1 つ選択する必要があります（たとえば、rsa-export1024-with-rc4-56-sha）。 通常、56 ビット ブラウザがこれらの暗号のうちの 1 つを送信する場合、両方が送信されるため、問題にはなりません。 ここでは、強力な暗号の残りを設定することができますが、暗号（rsa-with-rc4-128-sha）の重みが最も高くなるように重み付けをする必要があります。 他の強力な暗号に次に強力な重みを割り当て、エクスポート暗号には最低の重みを割り当てます。 次に、この設定がどのようなものかの例を示します（デフォルトが 1 であるため、エクスポート暗号には重みはありません）。

注: この例では、使用するエクスポート暗号スイートについて 2 つのオプションがあります。 シスコでは、どちらを使用するかは推奨できません。 ビジネス セキュリティの要件に基づいて決定

する必要があります。

解決策 1

エクスポート暗号（rsa-export1024-with-rc4-56-sha）を使用する場合、プロキシ リストは次のようになります。

- ssl-server 5 cipher rsa-with-rc4-128-sha 198.22.124.134 20094 weight 10
- ssl-server 5 cipher rsa-with-rc4-128-md5 198.22.124.134 20094 weight 8
- ssl-server 5 cipher rsa-with-des-cbc-sha 198.22.124.134 20094 weight 8
- ssl-server 5 cipher rsa-with-3des-ede-cbc-sha 198.22.124.134 20094 weight 8
- ssl-server 5 cipher rsa-export1024-with-rc4-56-sha 198.22.124.134 20094 weight 1

解決策 2

もう 1 つのエクスポート暗号（rsa-export1024-with-des-cbc-sha）をサポートする場合は、重み付けは次のようになります。

- ssl-server 5 cipher rsa-with-des-cbc-sha 198.22.124.134 20094 weight 10
- ssl-server 5 cipher rsa-with-rc4-128-sha 198.22.124.134 20094 weight 8
- ssl-server 5 cipher rsa-with-rc4-128-md5 198.22.124.134 20094 weight 8
- ssl-server 5 cipher rsa-with-3des-ede-cbc-sha 198.22.124.134 20094 weight 8
- ssl-server 5 cipher rsa-export1024-with-des-cbc-sha 198.22.124.134 20094 weight 1

関連情報

- CSS による SSL トラフィックの設定
- テクニカルサポート - Cisco Systems