無効なSSL設定によるSMAからのWSAアップグレードの失敗

内容

問題

SMA（セキュリティ管理アプライアンス）からWSA（Webセキュリティアプライアンス）をアップグレードしようとすると、アップグレードプロセスが失敗し、エラーメッセージ「Update failed to upgrade (Reason: Invalid SSL configuration)」が表示されます。 アップグレードはWSA Webインターフェイスから直接実行すると成功しますが、SMAから開始すると失敗します。新しい自己署名証明書を生成し、既定の認証証明書を変更して問題を解決しようとしましたが、失敗しました。

環境

- Cisco Web セキュリティ アプライアンス（WSA）
- ソフトウェアバージョン：15.2.2-009(MD)
- Cisco セキュリティ管理アプライアンス（SMA）
- ターゲットアップグレードバージョン：AsyncOS 15.5
- DNS機能が確認され、正常に動作している

解決方法

この問題を解決するには、WSAアプライアンスのレガシーTLSバージョン（TLSv1.0およびTLSv1.1）を無効にして、AsyncOS 15.5のアップグレードの前提条件を満たす必要があります。

ステップ1：根本原因の特定

このアップグレードの失敗は、AsyncOS 15.5の動作の変更によって発生します。この動作では、プロキシ設定以外のSSL設定でTLSv1.0とTLSv1.1はサポートされていません。このアップグレードプロセスでは、非プロキシSSL構成にTLSv1.2以降が必要です。

ステップ2：レガシーTLSバージョンを無効にする

WSAアプライアンスのTLSv1.0およびTLSv1.1を設定インターフェイスで無効にします。この変更はアップグレードの前提条件を満たし、アップグレードプロセスを続行できます。

ステップ3：外部サービスの互換性の確認

LDAPなどの外部サービスがTLSv1.2以降のバージョンをサポートしていることを確認します。これらのサービスがTLSv1.2以降と互換性がある限り、アップグレードによって外部システムとの通信が中断されることはありません。

ステップ4：アップグレードの続行

レガシーTLSバージョンを無効にした後、SMAからアップグレードプロセスを再試行します。これで、「Invalid SSL configuration（無効なSSL設定）」エラーなしでアップグレードを続行できます。

手順5：監視と検証

アップグレードプロセスを監視して、正常に完了したことを確認し、アップグレード後もTLSv1.2で依存するすべてのサービスが引き続き適切に機能することを検証します。

原因

このアップグレードの失敗は、AsyncOS 15.5.0-566で導入された動作変更によって引き起こされます。この動作変更では、プロキシ設定以外のSSL設定でTLSv1.0およびTLSv1.1がサポートされなくなりました。これにより、AsyncOSをアップグレードする前にTLSバージョンをTLSv1.2以降に変更する必要があるアップグレード前提条件が作成されます。SMAアップグレードプロセスでは、この非互換性を検出してアップグレードを続行できないようにするアップグレード前検証チェックが実行されます。

関連コンテンツ

- AsyncOS 15.5リリースノート
- 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。