AsyncOSのアップグレード後にTLSバージョン1.0が無効になる理由

内容

概要

このドキュメントでは、Transport Layer Security(TLS)バージョン1.0がアップグレード後にAsyncOSによって自動的に無効になる理由について説明します。

AsyncOSのアップグレード後にシスコがTLSバージョン1.0を無効にするのはなぜですか。

AsyncOS 9.5リリース以降、シスコはTLSv1.1およびv1.2機能を導入しました。以前は、TLSv1.0は古いプロトコルを必要とする環境のアップグレード後も有効なままですが、シスコではセキュアEメール環境の標準プロトコルとしてTLSv1.2に移行することを強く推奨しています。

Cisco AsyncOS 13.5.1以降のリリースでは、Cisco Secure Emailユーザのリスクを軽減するため、TLSバージョン1.0はシスコのセキュリティポリシーに従ってアップグレード時に自動的に無効になります。

これは以前、13.5.1 GDのリリースノート(リリースノート)で概説されています

SSL Configuration Changes	The following are the new changes made to SSL configuration settings: • There is no support for SSLv2 and SSL v3 methods. • There is no support for the TLS v1.0 method if your appliance is in the FIPS mode. • The TLS v1.0 method is disabled by default if your appliance is in the non-FIPS mode. • You can enable the TLS v1.0 method for the TLS client services (LDAP and Updater) in any one of the following ways: – System Administration > SSL Configuration page of the web interface of your appliance. See the "System Administration" section in the user guide – `sslconfig` command in the CLI. See the "CLI Reference Guide for AsyncOS 13.5.1 for Cisco Email Security Appliances." **Note** If you plan to upgrade from a lower AsyncOS version (for example, 12.x) in non-FIPS mode with TLS v1.0 enabled, to AsyncOS 13.5.1 and later, then TLS v1.0 is disabled by default. You need to enable the TLS v1.0 method on your appliance after upgrade.

13.5.1リリース以降の任意のバージョンのリリースにアップグレードすると、WebUIおよびコマンドライン(CLI)にも警告メッセージが表示されます。

After you upgrade to AsyncOS 13.5.1 and later, TLS v1.1 and v1.2 is enabled by default. - You cannot use TLS v1.0 in FIPS mode. - The appliance disables TLS v1.0 in non-FIPS mode after the upgrade but you can re-enable it if required.

> 警告:TLSv1.0を有効にすると、環境が潜在的なセキュリティリスクと脆弱性にさらされる可能性があります。シスコでは、データの安全な伝送を確保するために、使用可能なTLSv1.2および高暗号を使用することを強く推奨します。

現在、AsyncOS 15.0と同様に、Cisco Secure Email AsyncOSでは、アップグレード後にシステム管理者が自分の責任でTLSv1.0を再度有効にできます。これは、古いバージョン1.0プロトコルによって引き起こされる潜在的なセキュリティリスクが原因です。

この柔軟性は、今後のリリースで変更される可能性があり、今後のリリースでTLSv1.0を使用するオプションが削除されます。

TLSv1.0のセキュリティリスクと脆弱性：

SSLv3.0/TLSv1.0プロトコルの脆弱なCBCモードサーバ側の脆弱性(BEAST)
SSL/TLSv1.0 CRIME脆弱性

関連情報

- Cisco Secure Emailリリースノート
- テクニカル サポートとドキュメント - Cisco Systems
- Cisco Secure EmailでのTLSv1.0の有効化

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。