Pourquoi TLS version 1.0 est-il désactivé après la mise à niveau d'AsyncOS ?

Table des matières

Introduction

Ce document décrit la raison pour laquelle la version 1.0 de TLS (Transport Layer Security) est automatiquement désactivée par AsyncOS après les mises à niveau.

Pourquoi Cisco désactive-t-il TLS version 1.0 après la mise à niveau d'AsyncOS ?

Cisco a introduit les fonctionnalités TLSv1.1 et v1.2 depuis la version 9.5 d'AsyncOS. Auparavant, TLSv1.0 restait activé après les mises à niveau pour les environnements qui nécessitaient les protocoles plus anciens. Toutefois, Cisco a fortement encouragé le passage à TLSv1.2 en tant que protocole standard pour l'environnement de messagerie sécurisée.

À partir de la version 13.5.1 de Cisco AsyncOS, la version 1.0 de TLS est automatiquement désactivée lors de la mise à niveau conformément aux politiques de sécurité Cisco afin de réduire les risques pour les utilisateurs de la messagerie sécurisée Cisco.

Cela a déjà été décrit dans les notes de version de la version 13.5.1 GD (notes de version)

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.

Un message d'avertissement s'affiche également dans l'interface utilisateur Web et la ligne de commande (CLI) lors de la mise à niveau vers une version ultérieure à la version 13.5.1 :

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.

> Avertissement : l'activation de TLSv1.0 expose votre environnement à des risques et vulnérabilités potentiels. Cisco recommande vivement d'utiliser les algorithmes de chiffrement TLSv1.2 et élevé disponibles pour garantir la transmission sécurisée des données.

Actuellement, comme dans AsyncOS 15.0, Cisco Secure Email AsyncOS permet aux administrateurs système de réactiver TLSv1.0 après une mise à niveau à leurs propres risques en raison des risques de sécurité potentiels posés par les protocoles de l'ancienne version 1.0.

Cette flexibilité est susceptible d'être modifiée dans les versions ultérieures afin de supprimer l'option d'utilisation de TLSv1.0 dans les versions ultérieures.

Risques et vulnérabilités de sécurité avec TLSv1.0 :

Vulnérabilité côté serveur en mode CBC faible du protocole SSLv3.0/TLSv1.0 (BEAST)
Vulnérabilité SSL/TLSv1.0 CRIME

Informations connexes

- Notes de version de Cisco Secure Email
- Assistance et documentation techniques - Cisco Systems
- Activation de TLSv1.0 sur la messagerie sécurisée Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.