為什麼在AsyncOS升級後禁用TLS 1.0版

目錄

簡介

本文檔說明為什麼在升級後AsyncOS自動禁用傳輸層安全(TLS)版本1.0。

為什麼思科在AsyncOS升級後禁用TLS 1.0版？

自AsyncOS 9.5版本以來，思科推出了TLSv1.1和v1.2功能。以前，TLSv1.0在需要較舊協定的環境升級後處於啟用狀態，但思科強烈建議遷移到TLSv1.2作為安全電子郵件環境的標準協定。

從Cisco AsyncOS 13.5.1版本開始，TLS 1.0版在升級時根據思科安全策略自動禁用，以降低Cisco Secure Email使用者的風險。

之前在13.5.1 GD版本說明（版本說明）中對此進行了概述。

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.

升級到13.5.1版本之後的任何版本時，WebUI和命令列(CLI)中也會顯示警告消息：

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：啟用TLSv1.0會使您的環境面臨潛在的安全風險和漏洞。思科強烈建議使用可用的TLSv1.2和高級密碼來確保資料的安全傳輸。

目前，與AsyncOS 15.0一樣，Cisco Secure Email AsyncOS允許系統管理員在升級後重新啟用TLSv1.0，由於舊版本1.0協定可能帶來的安全風險，因此這些系統管理員需要自行承擔風險。

提供的這一靈活性在以後版本中可能會有所更改，以刪除以後版本中完全使用TLSv1.0的選項。

TLSv1.0的安全風險和漏洞：

SSLv3.0/TLSv1.0協定弱CBC模式伺服器端漏洞(BEAST)
SSL/TLSv1.0犯罪漏洞

相關資訊

- 思科安全電子郵件版本說明
- 技術支援與文件 - Cisco Systems
- 在思科安全電子郵件上啟用TLSv1.0

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。