为什么在AsyncOS升级后禁用TLS版本1.0

目录

简介

本文档说明为什么在升级后AsyncOS自动禁用传输层安全(TLS)版本1.0。

为什么思科在AsyncOS升级后禁用TLS版本1.0?

自AsyncOS 9.5版本以来，思科引入了TLSv1.1和v1.2功能。以前，TLSv1.0在需要较旧协议的环境升级后处于启用状态，但思科强烈建议迁移到TLSv1.2作为安全邮件环境的标准协议。

从Cisco AsyncOS 13.5.1版及更高版本开始，TLS 1.0版在升级时根据思科安全策略自动禁用，以降低思科安全邮件用户的风险。

之前在13.5.1 GD版本说明（版本说明）中对此进[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.

升级到13.5.1版本之后的任何版本时，WebUI和命令行(CLI)中也会显示警告消息：

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：启用TLSv1.0会使您的环境面临潜在的安全风险和漏洞。思科强烈建议使用可用的TLSv1.2和高密码来确保数据安全传输。

目前在AsyncOS 15.0,Cisco Secure Email AsyncOS允许系统管理员在升级后重新启用TLSv1.0，由于较旧版本1.0协议可能带来的安全风险，这些管理员会自行承担风险。

提供的这种灵活性在后来的版本中可能会有所变化，从而删除在以后的版本中完全使用TLSv1.0的选项。

TLSv1.0的安全风险和漏洞：

SSLv3.0/TLSv1.0协议弱CBC模式服务器端漏洞(BEAST)
SSL/TLSv1.0犯罪漏洞

相关信息

- 思科安全电邮版本说明
- 技术支持和文档 - Cisco Systems
- 在思科安全邮件上启用TLSv1.0

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。