Por que o TLS versão 1.0 está desabilitado após a atualização do AsyncOS

Contents

Introdução

Este documento descreve o motivo pelo qual o Transport Layer Security (TLS) versão 1.0 está sendo automaticamente desabilitado pelo AsyncOS após atualizações.

Por que a Cisco está desabilitando o TLS versão 1.0 após a atualização do AsyncOS?

A Cisco introduziu a funcionalidade TLSv1.1 e v1.2 desde as versões 9.5 do AsyncOS. Anteriormente, o TLSv1.0 era deixado habilitado após atualizações para ambientes que exigiam os protocolos mais antigos. No entanto, a Cisco incentivou fortemente a mudança para o TLSv1.2 como o protocolo padrão para o ambiente de e-mail seguro.

A partir da versão 13.5.1 do Cisco AsyncOS, o TLS versão 1.0 é desativado automaticamente na atualização de acordo com as políticas de segurança da Cisco para reduzir o risco para os usuários do Cisco Secure Email.

Isso foi descrito anteriormente nas notas de versão para 13.5.1 GD (**Notas de versão**)

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.

Uma mensagem de aviso também é exibida na WebUI e na linha de comando (CLI) ao atualizar para qualquer versão posterior à versão 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.

Aviso: a ativação do TLSv1.0 expõe seu ambiente a possíveis riscos e vulnerabilidades de segurança. A Cisco recomenda utilizar o TLSv1.2 e as cifras altas disponíveis para garantir a transmissão segura de dados.

Atualmente como no AsyncOS 15.0, o Cisco Secure Email AsyncOS permite que os administradores de sistema reabilitem o TLSv1.0 após a atualização por sua conta e risco devido aos possíveis riscos de segurança apresentados pelos protocolos da versão 1.0 mais antiga.

Essa flexibilidade oferecida está sujeita a alterações nas versões posteriores para remover a opção de utilizar o TLSv1.0 em todas as versões posteriores.

Riscos e vulnerabilidades de segurança com TLSv1.0:

Protocolo SSLv3.0/TLSv1.0 Vulnerabilidade do Lado do Servidor no Modo CBC Fraco (BEAST)
Vulnerabilidade de CRIME SSL/TLSv1.0

Informações Relacionadas

- **Notas da versão do Cisco Secure Email**
- **Suporte Técnico e Documentação - Cisco Systems**
- **Ativação do TLSv1.0 no Cisco Secure Email**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.