¿Por qué se inhabilita la versión 1.0 de TLS después de la actualización de AsyncOS?

Contenido

Introducción

Este documento describe el motivo por el cual la versión 1.0 de Transport Layer Security (TLS) está siendo deshabilitada automáticamente por AsyncOS después de las actualizaciones.

¿Por qué Cisco inhabilita la versión 1.0 de TLS después de la actualización de AsyncOS?

Cisco introdujo la funcionalidad TLSv1.1 y v1.2 desde las versiones 9.5 de AsyncOS. Anteriormente, TLSv1.0 se dejaba habilitado después de las actualizaciones para los entornos que requerían los protocolos más antiguos. Sin embargo, Cisco recomendaba encarecidamente pasar a TLSv1.2 como protocolo estándar para el entorno de correo electrónico seguro.

A partir de la versión 13.5.1 de Cisco AsyncOS y posteriores, la versión 1.0 de TLS se inhabilita automáticamente al actualizar según las políticas de seguridad de Cisco para reducir el riesgo para los usuarios de Cisco Secure Email.

Esto se describió anteriormente en las notas de la versión de 13.5.1 GD (**Notas de la versión**)

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.

También se muestra un mensaje de advertencia en la interfaz de usuario Web y en la línea de comandos (CLI) al actualizar a cualquier versión posterior a la 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.

Advertencia: la habilitación de TLSv1.0 expone su entorno a posibles riesgos y vulnerabilidades de seguridad. Cisco recomienda encarecidamente utilizar la versión TLSv1.2 y los cifrados altos disponibles para garantizar la transmisión segura de los datos.

Actualmente, como en AsyncOS 15.0, Cisco Secure Email AsyncOS permite a los administradores del sistema volver a habilitar TLSv1.0 después de la actualización bajo su propio riesgo debido a los riesgos potenciales de seguridad que plantean los protocolos de la versión anterior 1.0.

Esta flexibilidad que se ofrece está sujeta a cambios en versiones posteriores para eliminar la opción de utilizar TLSv1.0 en versiones posteriores.

Riesgos y vulnerabilidades de seguridad con TLSv1.0:

Vulnerabilidad del lado del servidor en modo CBC débil del protocolo SSLv3.0/TLSv1.0 (BEAST)
Vulnerabilidad CRIME de SSL/TLSv1.0

Información Relacionada

- **Notas de Cisco Secure Email Release**
- **Soporte Técnico y Documentación - Cisco Systems**
- **Habilitación de TLSv1.0 en Cisco Secure Email**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).