Why is TLS version 1.0 disabled after AsyncOS upgrade

Contents

Introduction

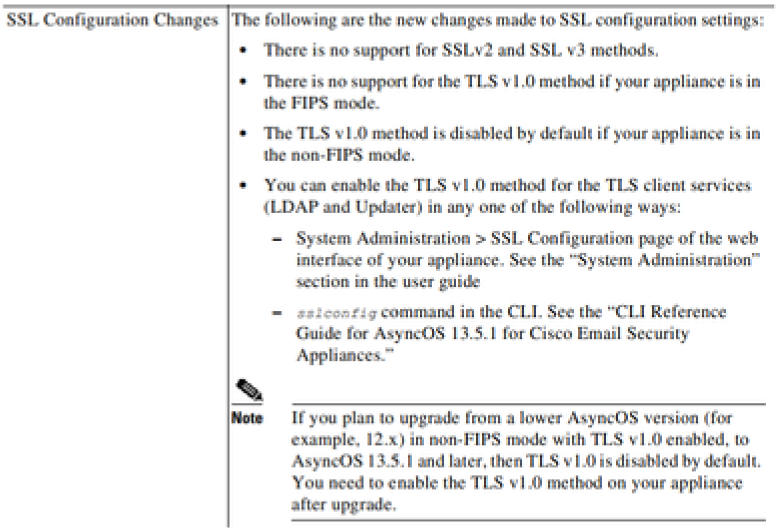
This document describes the reason why Transport Layer Security (TLS) version 1.0 is being automatically disabled by AsyncOS after upgrades.

Why is Cisco disabling TLS version 1.0 after AsyncOS upgrade?

Cisco introduced TLSv1.1 and v1.2 functionality since AsyncOS 9.5 releases. Previously, TLSv1.0 is left enabled after upgrades for environments that required the older protocols, however Cisco strongly encouraged moving to TLSv1.2 as the standard protocol for the Secure Email environment.

From Cisco AsyncOS 13.5.1 release and onwards, TLS version 1.0 is disabled automatically on upgrade per Cisco security policies to reduce the risk for the Cisco Secure Email users.

This was previously outlined in the release notes for 13.5.1 GD (**Release notes**)



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.

A warning message is also displayed in the WebUI and command line (CLI) when upgrading to any versions release after 13.5.1 release:

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.

> **Warning**: Enabling TLSv1.0 exposes your environment to potential security risks and vulnerabilities. Cisco highly recommends to utilise the available TLSv1.2 and high ciphers to ensure secured transmission of data.

Currently as at AsyncOS 15.0, Cisco Secure Email AsyncOS allows system administrators to re-enable TLSv1.0 after upgrade at their own risk due to the potential security risks posed by the older version 1.0 protocols.

This flexibility being offered is subject to change at latter releases to remove the option to utilise TLSv1.0 at all in later releases.

Security risks and vulnerabilities with TLSv1.0:

SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST)
SSL/TLSv1.0 CRIME Vulnerability

Related Information

- **Cisco Secure Email Release notes**
- **Technical Support & Documentation - Cisco Systems**
- **Enabling TLSv1.0 on Cisco Secure Email**