Perché TLS versione 1.0 è disabilitato dopo l'aggiornamento di AsyncOS

Sommario

Introduzione

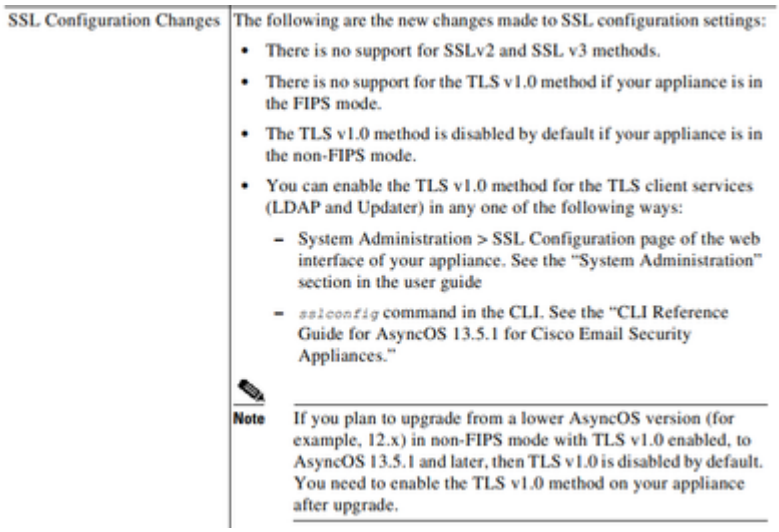
Questo documento descrive il motivo per cui Transport Layer Security (TLS) versione 1.0 viene disabilitato automaticamente da AsyncOS dopo gli aggiornamenti.

Perché Cisco disabilita TLS versione 1.0 dopo l'aggiornamento di AsyncOS?

Cisco ha introdotto le funzionalità di TLSv1.1 e v1.2 a partire dalle versioni AsyncOS 9.5. In precedenza, TLSv1.0 rimane abilitato dopo gli aggiornamenti per gli ambienti che richiedevano i protocolli precedenti. Cisco consiglia tuttavia di passare a TLSv1.2 come protocollo standard per l'ambiente di posta elettronica sicura.

A partire da Cisco AsyncOS versione 13.5.1, TLS versione 1.0 viene disabilitato automaticamente all'aggiornamento in base ai criteri di sicurezza Cisco per ridurre il rischio per gli utenti di Cisco Secure Email.

Questo concetto era già stato descritto nelle note di rilascio per la versione 13.5.1 GD (**note di rilascio**)



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.

Quando si esegue l'aggiornamento a qualsiasi versione successiva alla versione 13.5.1, viene visualizzato un messaggio di avviso anche nella WebUI e nella riga di comando (CLI):

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.

Avviso: l'abilitazione di TLSv1.0 espone l'ambiente a potenziali rischi e vulnerabilità di protezione. Cisco consiglia di utilizzare il protocollo TLSv1.2 disponibile e le cifrature ad alta velocità per garantire una trasmissione dei dati sicura.

Attualmente, come ad AsyncOS 15.0, Cisco Secure Email AsyncOS consente agli amministratori di sistema di riabilitare TLSv1.0 dopo l'aggiornamento a proprio rischio a causa dei potenziali rischi per la sicurezza posti dai protocolli della versione 1.0 meno recente.

Questa flessibilità è soggetta a modifiche nelle ultime versioni per rimuovere l'opzione di utilizzare TLSv1.0 nelle versioni successive.

TLSv1.0: rischi e vulnerabilità per la sicurezza:

Protocollo SSLv3.0/TLSv1.0 Vulnerabilità lato server modalità CBC debole (BEAST)
Vulnerabilità del codice SSL/TLSv1.0

Informazioni correlate

- **Note sulla release di Cisco Secure Email**
- **Documentazione e supporto tecnico â€“ Cisco Systems**
- **Abilitazione di TLSv1.0 su Cisco Secure Email**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).