Waarom is TLS versie 1.0 uitgeschakeld na AsyncOS upgrade

Inhoud

Inleiding

Dit document beschrijft de reden waarom Transport Layer Security (TLS) versie 1.0 automatisch wordt uitgeschakeld door AsyncOS na upgrades.

Waarom schakelt Cisco TLS versie 1.0 uit na een AsyncOS-upgrade?

Cisco introduceerde de functionaliteit TLSv1.1 en v1.2 sinds AsyncOS 9.5 releases. Voorheen werd TLSv1.0 ingeschakeld na upgrades voor omgevingen waarvoor de oudere protocollen nodig waren, maar Cisco heeft sterk aangeraden om over te stappen op TLSv1.2 als standaardprotocol voor de beveiligde e-mailomgeving.

Vanaf de release van Cisco AsyncOS 13.5.1 en daarna, wordt TLS versie 1.0 automatisch uitgeschakeld bij een upgrade per Cisco-beveiligingsbeleid om de risico's voor de beveiligde e-mailgebruikers van Cisco te verminderen.

Dit werd eerder beschreven in de opmerkingen bij de release voor 13.5.1 GD (**Releaseopmerkingen**)

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.

Er wordt ook een waarschuwingsbericht weergegeven in de WebUI- en opdrachtregel (CLI) bij het upgraden naar een versie van een versie na 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.

Waarschuwing: het inschakelen van TLSv1.0 stelt uw omgeving bloot aan mogelijke beveiligingsrisico's en kwetsbaarheden. Cisco raadt het gebruik van de beschikbare TLSv1.2 en hoge algoritmen ten zeerste aan om beveiligde gegevensoverdracht te waarborgen.

Op dit moment, zoals bij AsyncOS 15.0, stelt Cisco Secure Email AsyncOS systeembeheerders in staat om TLSv1.0 opnieuw in te schakelen na een upgrade op eigen risico vanwege de potentiële beveiligingsrisico's die worden gevormd door de oudere versie 1.0-protocollen.

Deze flexibiliteit die wordt aangeboden is onderhevig aan wijzigingen bij latere releases om de optie te verwijderen om TLSv1.0 te gebruiken in latere releases.

Beveiligingsrisico's en kwetsbaarheden met TLSv1.0:

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

Gerelateerde informatie

- **Opmerkingen over Cisco Secure E-mail release**
- **Technische ondersteuning en documentatie â€“ Cisco Systems**
- **TLSv1.0 inschakelen op Cisco Secure Email**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.