Warum ist TLS Version 1.0 nach dem AsyncOS-Upgrade deaktiviert?

Inhalt

Einleitung

In diesem Dokument wird der Grund beschrieben, warum Transport Layer Security (TLS) Version 1.0 von AsyncOS nach einem Upgrade automatisch deaktiviert wird.

Warum deaktiviert Cisco TLS Version 1.0 nach dem AsyncOS-Upgrade?

Seit der Einführung von AsyncOS 9.5 hat Cisco die Funktionen TLS v1.1 und v1.2 eingeführt. Bislang war TLSv1.0 nach Upgrades für Umgebungen, die ältere Protokolle erforderten, weiterhin aktiviert. Cisco empfahl jedoch nachdrücklich, TLSv1.2 als Standardprotokoll für die sichere E-Mail-Umgebung zu verwenden.

Ab Version Cisco AsyncOS 13.5.1 und darüber wird TLS Version 1.0 beim Upgrade automatisch gemäß den Cisco Sicherheitsrichtlinien deaktiviert, um das Risiko für Benutzer von Cisco Secure Email zu reduzieren.

Dies wurde bereits in den Versionshinweisen für 13.5.1 GD (**Versionshinweise)** beschrieben**.**

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.

Eine Warnmeldung wird auch in der WebUI und in der Befehlszeile angezeigt, wenn nach Version 13.5.1 ein Upgrade durchgeführt wird:

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.

Warnung: Durch die Aktivierung von TLSv1.0 besteht in Ihrer Umgebung ein erhöhtes Sicherheitsrisiko und es bestehen Schwachstellen. Cisco empfiehlt dringend, die verfügbaren TLSv1.2 und hohen Chiffren zu verwenden, um eine sichere Datenübertragung sicherzustellen.

Wie derzeit bei AsyncOS 15.0 ermöglicht Cisco Secure Email AsyncOS Systemadministratoren die erneute Aktivierung von TLSv1.0 nach dem Upgrade auf eigenes Risiko aufgrund der potenziellen Sicherheitsrisiken, die von älteren Protokollen der Version 1.0 ausgehen.

Diese Flexibilität kann sich bei späteren Versionen ändern, da TLSv1.0 in späteren Versionen nicht mehr verwendet werden kann.

Sicherheitsrisiken und Schwachstellen bei TLSv1.0:

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

Zugehörige Informationen

- **Cisco Secure Email Versionshinweise**
- **Technischer Support und Dokumentation für Cisco Systeme**
- **Aktivieren von TLSv1.0 auf Cisco Secure Email**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.