Collabra Mail

Dismissione protocolli TLS - FAQ

Versione 1.0
19 febbraio 2020

Dismissione protocolli TLS - FAQ

Introduzione

In seguito alla comunicazione inviata in data 14 Febbraio 2020 per notificare la dismissione delle versioni 1.0 e 1.1 del protocollo crittografico TLS, il supporto Collabra ha ricevuto una serie di richieste, molte delle quali sovrapponibili.
Lo scopo di questo documento è di rispondere a queste richieste.

Domande e risposte

Perché avete deciso di dismettere questi protocolli?

Le versioni 1.0 e 1.1 del protocollo crittografico TLS sono state dichiarate obsolete e "deprecated" dalla Internet Engineering Task Force(1), in quanto sono già stati vittime di diverse attacchi, risolti o mitigati negli ultimi anni, e potenzialmente esposti ad ulteriori gravi vulnerabilità in futuro.
Queste vulnerabilità sono conseguenza di debolezze intrinseche dell'implementazione degli algoritmi di cifratura che sono state risolte nella versione 1.2 e nella futura versione 1.3.

Alla luce di tutto questo la comunità Internazionale ha deciso di abbandonare l'utilizzazo delle versioni deboli del TLS nel 2015 dando alcuni anni di tempo agli sviluppatori software per aggiornare i loro prodotti almeno a TLS 1.2.
La scadenza ultima per la dismissione è prevista per il 9 Luglio 2020.

Tutti i maggiori produttori di software (Sistemi operativi, web browser, client di posta e framework di sviluppo) sono ad oggi compatibili con il TLS 1.2 ed elimineranno il supporto per le versioni 1.0 e 1.1 nel corso del 2020[2].

Visto che ormai ogni sistema client supporta il TLS 1.2 i service provider sono obbligati ad adeguarsi alle specifiche della IETF che richiedono di non proporre più le versioni 1.0 e 1.1 in fase di negoziazione della crittografia sui loro servizi.

In considerazione di tutto ciò e considerando anche che la reputazione dei propri server e servizi potrebbe avere una riduzione se il protocolli obsoleti rimangono disponibili, Collabra ha quindi deciso di implementare queste richieste e dismettere il supporto del TLS nelle versioni 1.0 e 1.1.

Potete rinviare questa operazione per darmi tempo di aggiornare i miei sistemi?

L'operazione di dismissione dei protocolli TLS obsoleti viene eseguita a livello di infrastruttura di posta, non è quindi possibile effettuarla selettivamente per singoli utenti o domini.
Inoltre questa riconfigurazione diventa inutile ai fini del mantenimento della qualità del servizio di posta elettronica se effettuata parzialmente o rimandata troppo a lungo.

Devo riconfigurare i miei client?

No. Se un client supporto il TLS 1.2 lo sta già utilizzando.
Se non lo supporta occorre aggiornalo ad una versione successiva.

Unica eccezione a questo riguarda alcune versione di Windows® e di applicazioni che girano su di esso. In questo caso il sistema operativo contiene il supporto per TLS 1.2, ma è disabilitato nelle configurazioni di default.
Le versioni di Windows® coinvolte sono quelle delle famiglie:
- Windows Server 2008
- Windows Server 2012
- Windows 7

per le quali occorre attivare esplicitamente il TLS 1.2[3].

Come posso verificare se i miei client sono compatibili?

Nella comunicazione del 14 Febbraio era riportato un elenco che indicava le versioni minime di sistemi operativi, browser, client di posta e framework di sviluppo che supportano TLS 1.2. Ogni versione più recente di quelle indicate è compatibile.

Se invece desiderate un controllo puntuale per il vostro browser potete consultare questa pagina web:
https://clienttest.ssllabs.com:8443/ssltest/viewMyClient.html

mentre quest'altra contiene un elenco più dettagliato dei browser e della loro compatibilità con TLS 1.2.

Per client di posta è più difficile effettuare una verifica puntuale, ma le ultime versioni dovrebbero essere compatibili e non creare nessun problema.
In particolare:

- outlook: utilizza le importazioni del sistema operativo quindi supporta il TLS 1.2 dalla versione 2010, ma in alcuni casi occorre abilitarlo (cfr.: "Devo riconfigurare i miei client")
- apple mail: essendo distribuito insieme a macOS è compatibile dalla versione 10.12 del sistema operativo (macOS Sierra)
- thunderbird: dalla versione 45.6 la compatibilità è completa, alcune versioni precedenti richiedono una riconfigurazione per il corretto funzionamento.
- altri: verificare con il produttore del client.

Inoltre in questa pagina:
https://luxsci.com/blog/tls-nist-cipher-email-web-browser-compatibility.html
è presente un altro elenco piuttosto dettagliata della compatibilità dei vari software.

Potrei fare un test di utilizzi di TLS 1.2 su Collabra?

Come detto sopra i servizi mail di Collabra forniscono già il supporto per TLS 1.2 e quindi se un client può utilizzarlo lo sta già facendo.

Potete fare una verifica sui miei client?

No, Collabra non è in grado di verificare i singoli client dei suoi clienti.
Per verificare i propri client fai riferimento a quando detto sopra.

Sto utilizzando un software che non supporta il TLS 1.2 cosa posso fare?

L'unica soluzione è aggiornare questi software a versioni più recenti.
Questa è un'attività che andrebbe comunque sempre effettuata per mantenere sicuri i tuoi dati, le tue comunicazioni e la tua identità in quanto i sistemi vecchi sono maggiormente vulnerabili e mettono a rischio la tua sicurezza.

Note

(1) https://tools.ietf.org/id/draft-ietf-tls-oldversions-deprecate-06.html
(2) https://www.thesslstore.com/blog/apple-microsoft-google-disable-tls-1-0-tls-1-1/
(3) https://support.microsoft.com/it-it/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-default-secure-protocols-in-wi

Indice