Ukončení podpory protokolů TLS 1.0 a TLS 1.1 u komunikačního rozhraní VREP/APEP pro zasílání e-Podání.

V současné době je v souvislosti s šifrovacími protokoly TLS 1.0 a 1.1 známo mnoho technických zranitelností, které mohou ohrozit informační systémy. Útočník v pozici „Man-in-the-Middle" může provést útok na přenášená šifrovaná data. Může potenciálně dešifrovat a následně odposlechnout elektronickou komunikaci. Proto se od použití těchto protokolů ustupuje s tím, že lze komunikovat přes protokol TLS 1.2.

ČSSZ, jakožto moderní úřad podporující elektronickou komunikaci se svými klienty, musí eliminovat případné hrozby související s provozováním starších protokolů TLS. Kybernetický útok na vzájemnou komunikaci mezi ČSSZ a jejím klientem s úmyslem narušit integritu a důvěrnost této komunikace by mohl významným způsobem omezit, nebo dokonce znemožnit poskytování služeb e-Podání. Proto ČSSZ rozhodla o ukončení podpory protokolů TLS 1.0 a TLS 1.1 u komunikačního rozhraní VREP/APEP pro příjem e-Podání k 31.12.2017. V produkčním prostředí VREP/APEP bude od 1.1.2018 podporován pouze komunikační protokol TLS 1.2.

ČSSZ si uvědomuje závažnost svého rozhodnutí, které ovlivní zejména uživatele starších operačních systémů (Windows XP, Vista) a neaktualizovaných SW pro zasílání e-Podání. Právě proto dává dostatečný prostor vývojářům a SW firmám pro přechod k zabezpečené komunikaci u jejího komunikačního rozhraní VREP/APEP prostřednictvím protokolu TLS 1.2 dle tohoto harmonogramu:

15.9.2017 V testovacím prostředí bude ukončena podpora protokolů TLS 1.0 a TLS 1.1 na komunikačních rozhraních:

- t-epodani.cssz.cz,
- vrep2-t.cssz.cz.

Podpora protokolů TLS 1.0 a TLS 1.1 bude ponechána pouze u komunikačního rozhraní:

- vrep1-t.cssz.cz (z důvodu testování rozhraní a jeho kompatibility).

Produkční prostředí zůstává do konce roku 2017 beze změny.

30.11.2117 Ukončení podpory TLS 1.0 a 1.1 v testovacím prostředí také u komunikačního rozhraní:

- vrep1-t.cssz.cz.

Celé testovací prostředí ČSSZ tak bude podporovat pouze komunikaci s TLS 1.2.
Produkční prostředí bude podporovat TLS 1.0, 1.1, 1.2 do 31.12.2017.

31.12.2017 Ukončení podpory TLS 1.0 a 1.1 v produkčním prostředí a to na všech komunikačních rozhraních VREP/APEP:

- epodani.cssz.cz,
- vrep1.cssz.cz,
- vrep2.cssz.cz.

Produkční prostředí bude od 1.1.2018 podporovat pouze TLS 1.2.

Jsme přesvědčeni, že klienti pochopí nezbytnost tohoto opatření, které vede k zajištění vyšších bezpečnostních standardů komunikace mezi ČSSZ a jejími klienty. Zároveň věříme že, SW vývojáři a SW firmy včas zareagují a poskytnou svým klientům SW komunikující s ČSSZ na dnešní době odpovídajících bezpečnostních standardech.