



Bern

12 gennaio 2015

Disattivazione del protocollo crittografico SSL v3 per internet

Bug di sicurezza "POODLE"

Gentile cliente,

Il bug di sicurezza "Poodle" permette di attaccare trasmissioni criptate con il protocollo SSL v3.

Per questo motivo a partire da inizio maggio saranno accettate solo trasmissioni con protocollo TLS versione 1.0 o superiore.

Qualora inviate tuttora in e-dec trasmissioni criptate con SSL v3, siete tenuti entro il 28.04.2015 ad aggiornare il protocollo al tipo TLS 1.0 oppure superiore.

Per permettervi di testare la nuova configurazione del vostro sistema, attiveremo un nuovo URL test temporaneo per l'ambiente e-dec test.

Sarà nostra premura informarvi non appena quest'ultimo sarà disponibile.

Nel caso sussistano incertezze, i clienti finali quali ad es. spedizionieri, esportatori ecc., sono pregati di rivolgersi al proprio fornitore del software / di prestazioni.

Cordiali saluti

Helpdesk CSC