Security Standards Council



SUPPLEMENTO INFORMATIVO

Migrazione da SSL e TLS iniziale

Versione 1.1
Data: Aprile 2016
Autore: Ente responsabile degli standard di protezione PCI

Riepilogo esecutivo

È giunto il momento di eseguire la migrazione.

Da oltre 20 anni SSL (Secure Sockets Layer) è presente nel mercato come uno dei protocolli di cifratura più ampiamente utilizzati mai rilasciati ed è fortemente diffuso ancora oggi, nonostante diverse vulnerabilità della sicurezza esposte nel protocollo.

SSL v3.0 è stato sostituito nel 1999 da TLS v1.0, che è stato a sua volta sostituito da TLS v1.1 e v1.2. A oggi, SSL e TLS iniziale non soddisfano più gli standard di sicurezza minimi a causa di vulnerabilità della sicurezza nel protocollo per le quali non esistono correzioni. È essenziale che le entità eseguano l'aggiornamento a un'alternativa sicura il prima possibile e disabilitino l'eventuale fallback a SSL e TLS iniziale.

SSL/TLS iniziale è stato rimosso come esempio di crittografia avanzata in PCI DSS v3.1 (aprile 2015).

Qual è il rischio?

SSL/TLS esegue la cifratura di un canale tra due endpoint (ad esempio, tra un browser Web e un server Web) per fornire privacy e affidabilità dei dati trasmessi sui canali di comunicazione. Dal rilascio di SSL v3.0, sono state identificate diverse vulnerabilità, più di recente alla fine del 2014 quando i ricercatori hanno pubblicato dettagli su una vulnerabilità della sicurezza (CVE-2014-3566) che può consentire agli aggressori di estrarre dati da connessioni sicure. Più comunemente definita POODLE (Padding Oracle On Downgraded Legacy Encryption), questa vulnerabilità è un attacco man-in-the-middle per cui è possibile decifrare un messaggio cifrato protetto da SSL v3.0.

Il protocollo SSL (tutte le versioni) non può essere corretto; non esistono metodi noti per risolvere le vulnerabilità come POODLE. SSL e TLS iniziale non soddisfano più le esigenze di sicurezza di entità che implementano la crittografia avanzata per proteggere i dati relativi ai pagamenti su canali di comunicazione pubblici o non attendibili. Inoltre, i moderni browser Web hanno iniziato a proibire le connessioni SSL, a impedire agli utenti di questi browser di accedere ai server Web che non hanno eseguito la migrazione a un protocollo più moderno.

Come rispondere?

La migliore risposta è disabilitare interamente SSL ed eseguire la migrazione a un protocollo di cifratura più moderno, che al momento della pubblicazione è almeno TLS v1.1, sebbene le entità siano fortemente incoraggiate a prendere in considerazione TLS v1.2. Tenere presente che non tutte le implementazioni di TLS v1.1 sono considerate sicure. Per istruzioni sulle configurazionI TLS sicure, fare riferimento a NIST SP 800-52 rev 1.

Implicazioni per PCI DSS

Per PCI DSS v3.1, SSL e TLS non sono più esempi di protocolli sicuri o crittografia avanzata. I requisiti PCI DSS direttamente interessati sono:

Requisito 2.2.3	Implementare funzioni di sicurezza aggiuntive per eventuali servizi, protocolli o daemon richiesti considerati non sicuri.
Requisito 2.3	Eseguire la cifratura di tutto l'accesso amministrativo non da console tramite crittografia avanzata.
Requisito 4.1	Utilizzare protocolli di sicurezza e crittografia avanzata per proteggere i dati sensibili dei titolari di carta durante la trasmissione su reti pubbliche e aperte.

SSL e TLS iniziale non devono essere utilizzati come controllo di sicurezza per soddisfare questi requisiti. Per supportare le entità nell'eseguire la migrazione da SSL/TLS iniziale, sono incluse le seguenti disposizioni:

- le nuove implementazioni non devono utilizzare SSL o TLS iniziale come controllo di sicurezza (nella sezione successiva vengono fornite istruzioni su implementazioni nuove ed esistenti);
- tutti i provider di servizi devono fornire un'offerta di servizio TLS sicura entro il 30 giugno **2016**;
- dopo il 30 giugno **2018**, tutte le entità devono aver interrotto l'utilizzo di SSL/TLS iniziale come controllo di sicurezza e utilizzare solo versioni sicure del protocollo (una concessione per alcuni terminali POI POS è descritta nell'ultimo punto elenco riportato di seguito);
- prima del 30 giugno 2018, le implementazioni esistenti che utilizzano SSL e/o TLS iniziale devono avere adottato un piano formale di migrazione e riduzione dei rischi;
- i terminali POI POS (e i punti di terminazione SSL/TLS a cui si connettono) che possono essere verificati come non soggetti a eventuali exploit noti per SSL e TLS iniziale possono continuare a utilizzare questi protocolli come controllo di sicurezza dopo il 30 giugno 2018.

Se si utilizza SSL/TLS iniziale, si applicano i requisiti dell'Appendice A2 PCI DSS "*Requisiti PCI DSS aggiuntivi per entità che utilizzano SSL/TLS iniziale*".

Informazioni su implementazioni "nuove" ed "esistenti"

Le implementazioni sono considerate "nuove" quando non c'è una dipendenza esistente dall'uso di protocolli vulnerabili. Scenari di esempio che sono considerati implementazioni "nuove" includono:

- installazione di un sistema in un ambiente che attualmente utilizza solo protocolli sicuri;
- installazione di un'applicazione in un sistema che attualmente utilizza solo protocolli sicuri;
- creazione di un nuovo sistema o rete per comunicare con altri sistemi/reti che supportano protocolli sicuri.

Se un'implementazione nuova non deve supportare un uso pre-esistente di un protocollo vulnerabile, deve essere eseguita solo con protocolli sicuri e crittografia avanzata ed essere configurata per non consentire il fallback al protocollo vulnerabile.

Nota: *le nuove implementazioni di e-commerce non devono considerare i browser Web per consumatori come infrastruttura pre-esistente che deve essere supportata.*

Invece, le implementazioni "esistenti" sono quelle con una dipendenza pre-esistente da, o un uso pre-esistente di, protocolli vulnerabili. Scenari di esempio che sono considerati implementazioni "esistenti" includono:

- installazione di un sistema in un ambiente che attualmente utilizza e/o ha l'esigenza di supportare protocolli vulnerabili;
- installazione di un'applicazione in un sistema che attualmente utilizza e/o ha l'esigenza di supportare protocolli vulnerabili;
- creazione di un nuovo sistema o rete per comunicare con altri sistemi/reti che attualmente utilizzano protocolli vulnerabili.

Si consiglia di aggiornare immediatamente le implementazioni esistenti, poiché l'uso continuativo di SSL/TLS iniziale potrebbe mettere a rischio l'ambiente.

Preparazione di un piano di migrazione e di riduzione dei rischi

Il piano di migrazione e riduzione dei rischi è un documento preparato dall'entità che illustra in maniera dettagliata i suoi piani per la migrazione a un protocollo sicuro e descrive anche i controlli che l'entità ha adottato per ridurre i rischi associati a SSL/TLS iniziale finché non viene completata la migrazione. Il piano di migrazione e riduzione dei rischi dovrà essere fornito al valutatore come parte del processo di valutazione PCI DSS.

Di seguito sono fornite istruzioni ed esempi di informazioni da documentare nel piano di migrazione e riduzione dei rischi:

- descrizione di come sono utilizzati i protocolli vulnerabili, inclusi;
    - il tipo di ambiente dove sono utilizzati i protocolli, ad esempio il tipo di canale di pagamento e le funzioni per cui sono utilizzati i protocolli;
    - il tipo di dati trasmessi, ad esempio elementi dei dati di account della carta di pagamento, connessioni di amministrazione, ecc.;
    - numero e tipi di sistemi che utilizzano e/o supportano i protocolli, ad es. terminali POI POS, switch di pagamento, ecc.
- risultati della valutazione dei rischi e controlli per la riduzione dei rischi in atto;

  - le entità devono aver valutato e documentato il rischio per il loro ambiente e aver implementato controlli per la riduzione dei rischi al fine di ridurre il rischio finché i protocolli vulnerabili non possono essere completamente rimossi.
- descrizione dei processi implementati per ricercare eventuali nuove vulnerabilità associate a protocolli vulnerabili:
  - Le entità devono essere proattive e restare informate sulle nuove vulnerabilità. Quando vengono pubblicate nuove vulnerabilità, l'entità deve valutare il rischio che esse rappresentano per il loro ambiente e determinare se devono essere implementati controlli aggiuntivi per la riduzione dei rischi finché la migrazione non è stata completata.
- descrizione dei processi di controllo delle modifiche implementati per assicurarsi che SSL/TLS iniziale non venga implementato nei nuovi ambienti;
  - Se un'entità attualmente non utilizza o non deve supportare protocolli vulnerabili, non esiste alcun motivo per introdurre tali protocolli nel suo ambiente. I processi di controllo delle modifiche includono la valutazione dell'impatto della modifica per confermare che tale modifica non introduce un nuovo punto debole della sicurezza nell'ambiente.
- panoramica del piano del progetto di migrazione inclusa la data di completamento della migrazione prevista non oltre il 30 giugno 2018:
  - La documentazione della pianificazione della migrazione include l'identificazione di quali sistemi/ambienti vengono migrati e quando, nonché la data prevista entro cui verrà completata la migrazione complessiva. La data prevista per la migrazione complessiva deve essere entro il 30 giugno 2018.

FAQ

Cosa sono i controlli per la riduzione dei rischi?

Per ambienti che attualmente utilizzano protocolli vulnerabili, l'implementazione e l'uso continuato di controlli per la riduzione dei rischi consentono di proteggere l'ambiente vulnerabile finché non viene completata la migrazione a un'alternativa sicura.

Alcuni controlli che possono essere utili per la riduzione dei rischi includono, senza limitazioni:

- riduzione della superficie dell'attacco il più possibile, mediante il consolidamento delle funzioni che utilizzano protocolli vulnerabili in un minor numero di sistemi e la riduzione del numero di sistemi che supportano i protocolli;
- rimozione o disabilitazione dell'uso di browser Web, JavaScript e cookie di sessione con effetti sulla sicurezza laddove non sono necessari;
- limitazione del numero di comunicazioni che utilizzano protocolli vulnerabili mediante il rilevamento e il blocco di richieste di downgrade a una versione di protocollo precedente;
- limitazione dell'uso di protocolli vulnerabili a entità specifiche, ad esempio, mediante la configurazione di firewall per consentire SSL/TLS iniziale solo in indirizzi IP noti (come partner aziendali che richiedono l'uso di protocolli) e il blocco di tale traffico per tutti gli altri indirizzi IP;
- miglioramento delle funzionalità di rilevamento/prevenzione mediante l'espansione della copertura di sistemi di protezione dalle intrusioni, l'aggiornamento di firme e il blocco dell'attività di rete che indica un comportamento pericoloso;
- monitoraggio attivo alla ricerca di attività sospette, ad esempio, identificazione di un insolito incremento di richieste di fallback a protocolli vulnerabili, e risposta appropriata.

Inoltre, le entità devono assicurarsi che anche tutti i requisiti PCI DSS applicabili siano in atto, inclusi:

- aggiornamento proattivo sulle nuove vulnerabilità, ad esempio, registrazione ai servizi di notifica delle vulnerabilità e ai siti di supporto dei fornitori per ricevere aggiornamenti sulle nuove vulnerabilità che emergono;
- applicazione dei consigli dei fornitori per la configurazione sicura delle loro tecnologie.

Quali sono alcune opzioni di migrazione?

Esempi di misure crittografiche aggiuntive che possono essere implementate e utilizzate come controllo di sicurezza per sostituire SSL/TLS possono includere:

- aggiornamento a una versione sicura corrente di TLS che viene implementata in modo sicuro e configurata per non accettare il fallback a SSL o TLS iniziale;
- cifratura di dati con crittografia avanzata prima di inviarli tramite SSL/TLS iniziale (ad esempio, uso di cifratura a livello di applicazione o di campo per cifrare i dati prima della trasmissione);
- impostazione iniziale di una sessione fortemente cifrata (ad es. tunnel IPsec) e invio dei dati tramite SSL in un tunnel sicuro.

Inoltre, l'uso dell'autenticazione a due fattori può essere combinata con i controlli riportati sopra per garantire l'autenticazione.

La scelta di un controllo crittografico alternativo dipenderà dalle esigenze tecniche e aziendali per un determinato ambiente.

Quali sono le caratteristiche degli ambienti dei piccoli esercenti?

Tutti i tipi di entità sono influenzati da problemi con SSL/TLS iniziale, inclusi i piccoli esercenti. È essenziale che i piccoli esercenti intraprendano le azioni necessarie per rimuovere SSL/TLS iniziale dal loro ambiente di dati dei titolari di carta per assicurarsi che i dati dei clienti siano sicuri.

Per l'ambiente POI, si consiglia ai piccoli esercenti di contattare il loro provider di terminali e/o acquirente (banca dell'esercente) per determinare se i loro terminali POI POS sono interessati dalle vulnerabilità SSL.

Per altri ambienti, ad es. terminali di pagamento virtuale, server di back-office, computer utente, ecc., i piccoli esercenti devono verificare se SSL/TLS iniziale viene utilizzato e dove è implementato, quindi determinare se un aggiornamento può essere eseguito immediatamente o se esiste una giustificazione aziendale per un aggiornamento ritardato (non oltre il 30 giugno 2018).

Suggerimenti per gli aspetti da prendere in considerazione nel proprio ambiente includono:

- controllo della versione del browser Web utilizzata nei sistemi (le versioni precedenti utilizzeranno SSL/TLS iniziale e potrebbe essere necessario eseguire l'aggiornamento a un browser più recente);
- controllo delle configurazioni dei firewall per verificare se è possibile bloccare SSL;
- controllo dell'aggiornamento di tutte le patch delle applicazioni e dei sistemi;
- controllo e monitoraggio dei sistemi per identificare eventuali attività sospette che possono indicare un problema della sicurezza.

Inoltre, durante la pianificazione della migrazione a un'alternativa sicura, è necessario completare un piano di migrazione e di riduzione dei rischi.

Come devono procedere gli esercenti con i terminali POI che supportano SSL/TLS iniziale?

I POI possono continuare a utilizzare SSL/TLS iniziale quando si può dimostrare che il POI non è soggetto agli exploit attualmente noti. Tuttavia, SSL è una tecnologia obsoleta e può essere soggetta a vulnerabilità della sicurezza aggiuntive in futuro; si consiglia pertanto di utilizzare TLS v1.1 o versione successiva negli ambienti POI laddove possibile. Per le nuove implementazioni di POI si consiglia di prendere in considerazione il supporto e l'uso di TLS 1.2 o versione successiva. Se SSL/TLS iniziale non è necessario nell'ambiente, si deve disabilitare l'utilizzo di e il fallback a queste versioni.

Quando si esaminano le implementazioni di terminali POI che utilizzano SSL/TLS iniziale, i valutatori devono rivedere la documentazione (ad esempio, documentazione fornita dal fornitore POI, dettagli di configurazione del sistema/della rete, ecc.) per determinare se l'implementazione è soggetta a exploit noti.

Se l'ambiente POI POS è soggetto a exploit noti, la pianificazione della migrazione a un'alternativa sicura deve iniziare immediatamente.

Nota: la concessione per i POI POS non attualmente soggetti agli exploit si basa sui rischi noti correnti. Se vengono introdotti nuovi exploit ai quali gli ambienti POI sono soggetti, gli ambienti POI dovranno essere aggiornati.

Perché gli ambienti POI POS sono meno vulnerabili?

PCI DSS fornisce una concessione per SSL e TLS iniziale affinché continuino a essere utilizzati dai dispositivi del punto di interazione (POI) del punto vendita (POS) e dai relativi punti di terminazione. Ciò si verifica perché le vulnerabilità note al momento della pubblicazione sono in generale più difficili da sfruttare in questi ambienti.

Ad esempio: alcune delle vulnerabilità SSL correnti vengono sfruttate da un aggressore che intercetta la comunicazione client/server e che manipola i messaggi al client. L'obiettivo dell'aggressore è portare il client a inviare dati aggiuntivi che l'aggressore può utilizzare per compromettere la sessione. I dispositivi POI POS con le seguenti caratteristiche sono in generale più resistenti a questo tipo di vulnerabilità:

- il dispositivo non supporta più connessioni lato client (il che facilita l'exploit POODLE);
- il protocollo di pagamento aderisce a ISO 20022 (Schema universale dei messaggi per il settore finanziario)/ISO 8583-1:2003 (Messaggi originati dalle carte delle transazioni finanziarie - Specifiche per lo scambio dei messaggi) o uno standard equivalente che limita la quantità di dati che possono essere esposti tramite "attacchi di di tipo replay";
- il dispositivo non utilizza software del browser Web, JavaScript o cookie di sessione relativi alla sicurezza.

Nota: queste caratteristiche sono solo a scopo esemplificativo; ciascuna implementazione dovrà essere valutata in modo indipendente per determinare l'estensione della suscettibilità alle vulnerabilità.

È anche importante ricordare che gli exploit continuano a evolvere e le organizzazioni devono essere preparate a rispondere alle nuove minacce. Tutte le organizzazioni che utilizzano SSL e/o TLS iniziale devono pianificare l'aggiornamento a un protocollo di crittografia avanzata il prima possibile.

Qualsiasi uso provvisorio di SSL/TLS iniziale in ambienti POI POS deve prevedere patch aggiornate e garantire che siano abilitate solo le estensioni necessarie.

Cosa significa questo per gli elaboratori pagamenti che supportano ambienti POI?

Le entità di tutti i tipi sono interessate dal problema di SSL/TLS iniziale, inclusi elaboratori pagamenti, gateway di pagamenti e altre entità che forniscono servizi di elaborazione delle transazioni. Queste entità dovranno esaminare il loro uso di SSL/TLS iniziale e pianificare migrazioni nello stesso modo delle altre entità.

Le entità che elaborano pagamenti con punti di terminazione POI dovranno verificare che le comunicazioni POI non siano vulnerabili (come descritto nella sezione "Perché gli ambienti POI POS sono meno vulnerabili?" riportata sopra) se devono continuare a utilizzare SSL/TLS iniziale.

Se un'entità che elabora pagamenti supporta più canali di pagamento, ad esempio transazioni di e-commerce e POI, nello stesso punto di terminazione, l'entità dovrà assicurarsi che tutti i canali vulnerabili vengano migrati a un'alternativa sicura entro il 30 giugno 2018. Se l'ambiente POI non è considerato soggetto a vulnerabilità, l'entità può prendere in considerazione le seguenti opzioni:

- migrare canali POI a un'alternativa sicura in modo che le transazioni di e-commerce e POI possano continuare a utilizzare lo stesso punto di terminazione;
- nel caso in cui i canali POI non vengano migrati, possono essere utilizzati interfacce/punti di terminazione separati per separare il traffico POI che utilizza SSL/TLS iniziale dal traffico di e-commerce che è stato migrato a un'alternativa sicura.

Quali sono le caratteristiche degli ambienti di e-commerce?

A causa della natura degli ambienti basati sul Web, le implementazioni di e-commerce presentano la massima suscettibilità e sono pertanto a rischio immediato di vulnerabilità note in SSL/TLS iniziale.

Per questo motivo, i nuovi siti Web di e-commerce non devono utilizzare o supportare SSL/TLS iniziale.

Gli ambienti di e-commerce con l'esigenza corrente di supportare clienti che utilizzano SSL/TLS iniziale devono iniziare la migrazione il prima possibile, completando tutte le migrazioni entro il 30 giugno 2018. Laddove non è possibile eseguire la migrazione immediatamente, la giustificazione deve essere documentata come parte del piano di migrazione e di riduzione dei rischi.

Finché non viene completata la migrazione, si consiglia di ridurre il numero di server che supportano SSL/TLS iniziale il più possibile. La riduzione del numero di sistemi vulnerabili riduce la potenziale esposizione a eventuali exploit e può anche semplificare i controlli per la riduzione dei rischi, come il miglioramento del monitoraggio del traffico sospetto.

Si consiglia inoltre agli esercenti di e-commerce di avvisare i loro clienti di aggiornare i browser Web per supportare protocolli sicuri.

Da dove iniziare con il processo di migrazione?

Di seguito sono riportati alcuni suggerimenti per aiutare le entità a pianificare la loro migrazione a un'alternativa sicura:

1. identificare tutti i componenti di sistema e flussi di dati che sono basati su e/o supportano i protocolli vulnerabili;
2. per ciascun componente di sistema o flusso di dati, identificare l'esigenza aziendale e/o tecnica per l'uso del protocollo vulnerabile;
3. rimuovere o disabilitare immediatamente tutte le istanze di protocolli vulnerabili che non presentano un'esigenza aziendale e/o tecnica di supporto;
4. identificare le tecnologie per sostituire i protocolli vulnerabili e documentare le configurazioni sicure da implementare;
5. documentare un piano del progetto di migrazione che definisca passaggi e tempi per gli aggiornamenti;
6. implementare i controlli per la riduzione dei rischi per ridurre la suscettibilità a exploit noti finché i protocolli vulnerabili non vengono rimossi dall'ambiente;
7. eseguire migrazioni e seguire procedure di controllo delle modifiche per assicurarsi che gli aggiornamenti dei sistemi siano testati e autorizzati;
8. aggiornare gli standard di configurazione del sistema al completamento delle migrazioni ai nuovi protocolli.

SSL/TLS iniziale può rimanere in un ambiente se non utilizzato come controllo di sicurezza?

Sì, questi protocolli possono restare in uso in un sistema purché non si utilizzi SSL/TLS iniziale come controllo di sicurezza.

Inoltre, tutte le vulnerabilità SSL/TLS con un punteggio CVSS 4 o superiore in una scansione ASV o classificate come "Elevate" in una scansione delle vulnerabilità interna dell'entità, devono essere risolte entro i tempi richiesti (ad es. trimestre per le scansioni ASV) al fine di soddisfare il Requisito 11.2 PCI DSS. Seguire processi di gestione delle vulnerabilità definiti per documentare come le vulnerabilità SSL/TLS vengono risolte, ad esempio, dove SSL/TLS iniziale viene utilizzato solo per le comunicazioni POI non soggette a exploit o dove è presente ma non viene utilizzato come controllo di sicurezza (ad es. non viene utilizzato per proteggere la riservatezza della comunicazione).

Le date della migrazione si applicano se non si sono verificate compromissioni dei dati dei titolari di carta derivanti dall'uso di SSL/TLS iniziale?

Sì, la data per la migrazione da SSL/TLS iniziale non è interessata dal numero di compromissioni di dati delle carte di pagamento che possono verificarsi o meno in futuro. I requisiti PCI DSS intendono impedire le compromissioni dei dati dei titolari di carta tramite un approccio di difesa in profondità. Aspettare che potenziali violazioni dei dati vengano pubblicizzate prima di intraprendere azioni per proteggere i propri dati non è un approccio alla sicurezza efficace e non è supportato in PCI DSS.

In che modo la presenza di SSL influisce sui risultati delle scansioni ASV?

SSL v3.0 e TLS iniziale contengono diverse vulnerabilità, alcune delle quali attualmente ottengono un punteggio di 4.3 nel CVSS (Common Vulnerability Scoring System). Il CVSS è definito come NVD (National Vulnerability Database) ed è il sistema di valutazione che gli ASV devono utilizzare. Tutte le vulnerabilità di rischio medio o elevato (ad es. le vulnerabilità con un CVSS di 4.0 o superiore) devono essere corrette e i sistemi interessati nuovamente sottoposti a scansione dopo le correzioni per mostrare che il problema è stato risolto.

Tuttavia, poiché non esiste un modo noto per risolvere alcune di queste vulnerabilità, si consiglia di eseguire la migrazione a un'alternativa sicura il prima possibile. Le entità che non sono in grado di eseguire immediatamente la migrazione a un'alternativa sicura devono collaborare con il loro ASV per documentare il loro determinato scenario come segue:

- *Prima del 30 giugno 2018:* le entità che non hanno completato la loro migrazione devono fornire all'ASV la conferma documentata che hanno implementato un piano di migrazione e di riduzione dei rischi e che stanno lavorando per completare la migrazione entro la data richiesta. La ricezione di questa conferma deve essere documentata dall'ASV come eccezione nel processo di eccezioni, falsi positivi e controlli compensativi del Riepilogo esecutivo del rapporto di scansione ASV e l'ASV può emettere il risultato di esito positivo per tale componente della scansione o host, se l'host soddisfa tutti i requisiti di scansione applicabili.
- *Dopo il 30 giugno 2018:* le entità che non hanno eseguito completamente la migrazione da SSL/TLS iniziale dovranno seguire il processo di risoluzione delle vulnerabilità con controlli compensativi per verificare che il sistema interessato non sia soggetto a quelle determinate vulnerabilità. Ad esempio, laddove SSL/TLS iniziale è presente ma non viene utilizzato come controllo di sicurezza (ad es. non viene utilizzato per proteggere la riservatezza della comunicazione).

Le entità con terminali POI POS e/o punti di terminazione che sono stati verificato come non soggetti alle vulnerabilità specifiche possono essere idonee per una riduzione nel punteggio NVD per tali sistemi. In questo scenario, l'ASV deve fornire (oltre a tutti gli altri elementi di reporting richiesti) le seguenti informazioni in conformità con la Guida del programma ASV:

- valutazione NVD della vulnerabilità;
- valutazione ASV della vulnerabilità;
- motivo del disaccordo dell'ASV con la valutazione NVD.

Ad esempio, l'ASV potrebbe determinare che una vulnerabilità specifica presenta una difficoltà maggiore da sfruttare in un determinato ambiente POI POS rispetto a quella definita dal sistema di valutazione NVD generale. L'ASV può quindi riclassificare questo elemento del sistema di valutazione per la vulnerabilità specifica, per i sistemi in questione.

Quando si apportano eventuali modifiche di questo tipo, l'ASV deve considerare l'ambiente, i sistemi e i controlli specifici del cliente e non eseguire tali modifiche in base a supposizioni o tendenze generali. Il cliente della scansione deve collaborare con l'ASV per fornire una descrizione del suo ambiente; altrimenti, l'ASV non sarà in grado di determinare se la modifica di un punteggio CVSS è appropriata.

Gli ASV devono esercitare la dovuta diligenza e la dovuta attenzione quando impiegano tali concessioni e assicurarsi che ci siano prove sufficienti per supportare un modifica del punteggio CVSS. Tutte queste modifiche devono seguire il processo definito nella Guida del programma ASV.

Tutti i rapporti di scansione ASV devono essere completati in conformità con la Guida del programma ASV.

Questo significa che le entità con un piano di migrazione e di riduzione dei rischi non devono applicare le patch per la correzione delle vulnerabilità in SSL/TLS iniziale?

No, le date della migrazione previste non sono una scusa per ritardare l'applicazione di patch per le vulnerabilità. Nuovi rischi e minacce devono continuare a essere gestiti in conformità con i Requisiti PCI DSS applicabili, come 6.1, 6.2 e 11.2, e le entità devono risolvere le vulnerabilità laddove è disponibile una patch, una correzione o un aggiornamento della sicurezza.

Qual è l'impatto per i servizi che supportano protocolli sicuri (ad es. TLS v1.2) e protocolli insicuri (ad es. SSL/TLS iniziale)?

Molti provider di servizi (ad esempio, provider di hosting condiviso) forniscono piattaforme e servizi per un'ampia base di clienti, che possono includere entità che devono soddisfare i requisiti PCI DSS come pure entità che non li soddisfano. I provider di servizi che supportano il CDE di un cliente possono dimostrare che soddisfano i requisiti applicabili per conto del cliente o che forniscono opzioni di

servizi che soddisfano i requisiti PCI DSS utilizzabili dai loro clienti. I provider di servizi devono chiaramente comunicare ai loro clienti quali protocolli di sicurezza sono offerti, come configurare le differenti opzioni e l'impatto dell'uso di configurazione considerate sicure.

Ad esempio, un provider di hosting Web può offrire una piattaforma Web ospitata per gli esercenti che supporta TLS v1.2 e anche protocolli più deboli. Per supportare la conformità agli standard PCI DSS dei loro clienti, i provider di hosting devono fornire chiare istruzioni per consentire al cliente di configurare il loro uso del servizio solo tramite TLS v1.2 senza fallback a SSL/TLS iniziale. Dal lato cliente, un esercente che utilizza questa piattaforma come parte della sua implementazione PCI DSS dovrà assicurarsi che le opzioni di configurazione che sta utilizzando includano TLS v1.2 senza fallback a SSL/TLS iniziale.

La presenza di protocolli più deboli in un ambiente di hosting misto può determinare un errore durante la scansione ASV. Quando ciò si verifica, il provider di servizi e l'ASV devono seguire il processo di eccezioni, falsi positivi e controlli compensativi per documentare come è stato risolto il rischio, ad esempio confermando che SSL/TLS iniziale non viene utilizzato come controllo di sicurezza dal provider di servizi e che vengono fornite al cliente opzioni di configurazione sicura non permettono il fallback a protocolli più deboli. L'ASV può quindi emettere il risultato di esito positivo per tale componente della scansione o host, se l'host soddisfa tutti i requisiti di scansione applicabili.