Security Standards Council

COMPLEMENT D'INFORMATIONS :

Migration depuis les protocoles SSL et TLS initial

Version 1.1
Date : Avril 2016
Auteur : Conseil des normes de sécurité PCI

Résumé

Le temps de migrer est arrivé.

Depuis plus de 20 ans, le protocole SSL (Secure Sockets Layer) était l'un des protocoles de cryptage les plus largement utilisés du marché, et l'est encore à l'heure actuelle malgré diverses vulnérabilités de sécurité reconnues.

Le protocole SSL v3.0 a été remplacé en 1999 par le protocole TLS v1.0, remplacé à son tour par le protocole TLS v1.1 et v1.2. À ce jour, les protocoles SSL et TLS initial ne respectent plus les normes de sécurité minimales en raison de vulnérabilités de sécurité pour lesquelles il n'existe aucun correctif. Il est essentiel que les entités adoptent une alternative sécurisée aussitôt que possible, et empêchent tout repli vers les protocoles SSL et TLS initial.

Les protocoles SSL/TLS initial ne sont plus des exemples de cryptographie robuste dans le cadre de la norme PCI DSS v3.1 (avril 2015).

Quel est le risque ?

Les protocoles SSL/TLS cryptent un canal entre deux points de terminaison (par exemple, entre un navigateur Web et un serveur Web) afin de garantir la confidentialité et la fiabilité des données transmises sur le canal de communications. Depuis la sortie du protocole SSL v3.0, plusieurs vulnérabilités ont été identifiées, dont la dernière en date remonte à la fin de 2014, lorsque des chercheurs publièrent les détails d'une vulnérabilité de sécurité (CVE-2014-3566) permettant à des pirates d'extraire des données à partir de connexions sécurisées. Cette vulnérabilité, plus connue sous le nom de POODLE (pour « Padding Oracle On Downgraded Legacy Encryption ») est une « attaque de l'homme du milieu » par laquelle il est possible de décrypter un message crypté sécurisé par SSL v3.0.

Le protocole SSL (toutes versions) ne peut être corrigé, mais certaines méthodes connues permettent de remédier aux vulnérabilités comme POODLE. Les protocoles SSL et TLS initial ne répondent plus aux besoins sécuritaires des entités qui implémentent une cryptographie robuste pour protéger leurs données de paiement sur les canaux de communications publics ou non fiables. En outre, les navigateurs Web modernes commencent à interdire les connexions SSL, empêchant les utilisateurs de ces navigateurs d'accéder aux serveurs Web n'ayant pas migré vers un protocole plus moderne.

Comment y répondre ?

La meilleure réponse est de désactiver entièrement le protocole SSL et de migrer vers un protocole de cryptage plus moderne. Au moment de cette publication, il s'agit au minimum du protocole TLS v1.1, bien que certaines entités soient fortement encouragées à envisager le protocole TLS v1.2. Notez que toutes les implémentations du protocole TLS v1.1 ne sont pas considérées comme sécurisées. Reportez-vous aux directives SP 800-52, Rév. 1 du NIST pour obtenir de l'aide sur les configurations TLS sécurisées.

Ce que cela signifie pour PCI DSS

D'après la norme PCI DSS v3.1, les protocoles SSL et TLS initial ne sont plus des exemples de cryptographie robuste ou de protocole sécurisé. Les conditions de la norme PCI DSS directement concernées sont les suivantes :

Condition 2.2.3	Implémentation des fonctions de sécurité supplémentaires pour tout service, protocole ou démon nécessaire et jugé comme non sécurisé.
Condition 2.3	Crypter tous les accès administratifs non console, à l'aide d'une cryptographie robuste.
Condition 4.1	Utiliser des protocoles de cryptographie et de sécurité robustes pour sauvegarder les données des titulaires de cartes sensibles lors de leur transmission sur des réseaux publics et ouverts.

Ne pas utiliser le SSL et le TLS initial en tant que contrôles de sécurité pour remplir ces conditions. Les mesures suivantes sont disponibles pour aider les entités à abandonner le SSL et le TLS initial :

- Les nouvelles implémentations ne doivent pas utiliser le SSL ou le TLS initial comme contrôle de sécurité (vous trouverez des informations sur les nouvelles implémentations et les implémentations existantes dans la prochaine partie).
- Tous les prestataires de services doivent proposer un service TLS sécurisé pour le 30 juin **2016**.
- Après le 30 juin **2018**, toutes les entités doivent avoir interrompu leurs recours au SSL/TLS initial en tant que contrôles de sécurité et utiliser exclusivement les versions sécurisées du protocole (le recours à certains terminaux POS POI est autorisé et décrit dans le dernier point ci-dessous).
- D'ici le 30 juin 2018, les implémentations existantes, qui utilisent le SSL et/ou le TLS initial, doivent comporter un plan formel d'atténuation des risques et de migration.
- Vous pouvez continuer à utiliser les terminaux POS POI (et les points de terminaisons SSL/TLS auxquels ils sont connectés) en tant que contrôles de sécurité après le 30 juin 2018 après vous être assuré qu'ils ne sont pas susceptibles d'occasionner des failles connues pour le protocole SSL ou TLS initial.

Si le protocole SSL/TLS initial est utilisé, les conditions de la norme PCI DSS, Annexe A2 (« *Autres clauses de la norme PCI DSS pour les entités utilisant le SSL/ TLS initial* ») s'appliqueront.

Comprendre les « nouvelles » implémentations et les implémentations « existantes »

Les implémentations sont considérées comme « nouvelles » lorsqu'il n'existe pas de dépendance pour l'utilisation des protocoles vulnérables. Quelques exemples de scénarios pouvant être considérés comme de « nouvelles » implémentations incluent :

- Installer un système dans un environnement n'utilisant actuellement que des protocoles sécurisés
- Installer une application dans un système n'utilisant actuellement que des protocoles sécurisés
- Construire un nouveau système ou un nouveau réseau pour communiquer avec d'autres systèmes/réseaux prenant en charge les protocoles sécurisés

Si une nouvelle implémentation ne nécessite pas la prise en charge d'une utilisation préexistante d'un protocole vulnérable, elle doit être implémentée uniquement avec des protocoles sécurisés et une cryptographie robuste, et être configurée afin de ne pas permettre de repli vers le protocole vulnérable.

Remarque : *les nouvelles implémentations de commerce électronique ne doivent pas considérer les navigateurs Web de consommateur comme une infrastructure préexistante devant être prise en charge.*

Inversement, les implémentations « existantes » sont celles où l'on utilise ou fait déjà confiance à des protocoles vulnérables. Quelques exemples de scénarios pouvant être considérés comme des implémentations « existantes » incluent :

- Installer un système dans un environnement utilisant actuellement et/ou ayant besoin de prendre en charge des protocoles vulnérables
- Installer une application dans un système utilisant actuellement et/ou ayant besoin de prendre en charge des protocoles vulnérables
- Construire un nouveau système ou un nouveau réseau pour communiquer avec d'autres systèmes/réseaux utilisant actuellement des protocoles vulnérables

Étant donné que l'utilisation prolongée du SSL/TLS initial peut faire courir un risque à l'environnement, il est recommandé de mettre immédiatement à niveau les implémentations existantes.

Préparer un plan d'atténuation des risques et de migration

Le plan d'atténuation des risques et de migration est un document préparé par l'entité qui détaille les projets de migration vers un protocole sécurisé, et décrit les contrôles de l'entité pour atténuer le risque associé au SSL/TLS initial tant que la migration n'est pas terminée. Le plan d'atténuation des risques et de migration devra être fourni à l'évaluateur dans le cadre du processus d'évaluation de la norme PCI DSS.

Voici quelques conseils et exemples d'informations à inclure dans le plan d'atténuation des risques et de migration :

- Une description de la façon dont les protocoles vulnérables sont utilisés, dont :

  - Le type d'environnement où les protocoles sont utilisés (par ex., le type de canal de paiement et les fonctions pour lesquelles les protocoles sont utilisés).
  - Le type de données transmises (par ex., des éléments de données de compte de carte de paiement, les connexions administratives, etc.).
  - Le nombre et les types de systèmes utilisant et/ou prenant en charge les protocoles (par ex., les terminaux POS POI, les commutateurs de paiement, etc.).
- Les résultats d'évaluation des risques et les contrôles d'atténuation des risques en vigueur :
  - Les entités doivent avoir évalué et documenté le risque pour leur environnement, et implémenté des contrôles d'atténuation des risques pour contribuer à atténuer le risque jusqu'à ce que les protocoles vulnérables puissent être complètement supprimés.
- Une description des processus implémentés pour surveiller les nouvelles vulnérabilités associées aux protocoles vulnérables :
  - Les entités doivent être proactives et rester informées des nouvelles vulnérabilités. Au fur et à mesure de la publication de nouvelles vulnérabilités, les entités doivent évaluer le risque que ces vulnérabilités représentent pour leur environnement, et déterminer si des contrôles d'atténuation des risques supplémentaires doivent être mis en place tant que la migration n'est pas complète.
- Une description des processus liés au contrôle de changement implémentés pour s'assurer que le SSL/TLS initial n'est pas implémenté dans les nouveaux environnements :
  - Si une entité n'utilise pas ou n'a pas besoin de prendre en charge les protocoles vulnérables pour le moment, elle n'a pas de raison d'introduire de tels protocoles dans son environnement. Les processus de contrôle de changement incluent l'évaluation de l'impact du changement, afin de s'assurer que le changement n'introduit pas de nouvelles failles de sécurité dans l'environnement.
- Un aperçu du plan de migration, y compris la date d'achèvement cible fixée au 30 juin 2018 au plus tard :
  - Les documents du plan de migration incluent l'identification des systèmes et environnements en voie de migration, les délais de leur migration, ainsi qu'une date cible pour laquelle la migration globale aura été effectuée. La date cible pour la migration globale doit être le 30 juin 2018 au plus tard.

Questions fréquentes

Que sont les contrôles d'atténuation des risques ?

Pour les environnements utilisant actuellement des protocoles vulnérables, l'implémentation et l'utilisation continue de contrôles d'atténuation des risques contribuent à protéger les environnements vulnérables tant que la migration vers une alternative sécurisée n'est pas complète.

Certains contrôles pouvant contribuer à l'atténuation des risques incluent, notamment :

- Minimiser autant que possible la surface d'attaque en consolidant les fonctions utilisant des protocoles vulnérables sur moins de systèmes, et diminuer le nombre de systèmes prenant en charge les protocoles.
- Supprimer ou empêcher l'utilisation des navigateurs Web, de JavaScript, et des cookies de session ayant un impact sur la sécurité lorsque ces éléments ne sont pas nécessaires.
- Restreindre le nombre de communications utilisant les protocoles vulnérables, en détectant et en bloquant les demandes de passage à une version de protocole antérieure.
- Restreindre l'utilisation des protocoles vulnérables à certaines entités spécifiques, par exemple, en configurant les pare-feu de manière à n'autoriser le SSL/TLS initial que pour les adresses IP connues (les partenaires commerciaux devant utiliser les protocoles, par exemple), et en bloquant ce trafic pour toutes les autres adresses IP.
- Améliorer la détection et la prévention des capacités en élargissant la couverture des systèmes de prévention d'intrusion, en mettant à jour les signatures, et en bloquant toute activité du réseau indiquant un comportement malicieux.
- Contrôler activement les activités suspicieuses, par exemple, en identifiant les augmentations inhabituelles de demandes de repli vers les protocoles vulnérables, et en répondant en conséquence.

En outre, les entités doivent s'assurer que toutes les exigences de la norme PCI DSS applicables sont en place, y compris :

- Rester au courant des nouvelles vulnérabilités de manière proactive, par exemple en s'abonnant à des services de notification des vulnérabilités et à des sites d'assistance aux vendeurs, afin de bénéficier de mises à jour sur les nouvelles vulnérabilités au moment où elles apparaissent.
- Demander à recevoir des conseils des vendeurs pour configurer leurs technologies de manière sécurisée.

Quelles sont certaines options de migration ?

Les moyens cryptographiques supplémentaires pouvant être mis en œuvre et utilisés comme contrôle de sécurité pour remplacer le SSL/TLS initial incluent :

- Passer à une version sécurisée et à jour du protocole TLS, implémenté de manière sécurisée et configuré pour refuser les replis vers le SSL ou le TLS initial.
- Crypter les données avec une cryptographie robuste avant de les envoyer via le protocole SSL/TLS initial (par exemple, en utilisant un cryptage au niveau du champ ou de l'application pour crypter les données avant leur transmission).
- Commencer par définir une session fortement cryptée (par exemple, un tunnel IPsec), puis envoyer les données via SSL au sein d'un tunnel sécurisé.

En outre, un système d'authentification à deux facteurs peut être associé aux contrôles ci-dessus pour garantir une authentification robuste.

Le choix d'un contrôle cryptographique alternatif dépendra des besoins techniques et commerciaux de chaque environnement.

Qu'en est-il des petits environnements commerçants ?

Tous les types d'entités sont influencés par les problèmes de SSL/TLS initial, y compris les petits commerçants. Les petits commerçants doivent absolument prendre les mesures nécessaires pour supprimer le SSL/TLS initial de leur environnement de données du titulaire, afin de garantir la sécurité des données de leurs clients.

Pour l'environnement POI, il est recommandé aux petits commerçants de contacter leur fournisseur de terminal et/ou l'acquéreur (la banque du commerçant) afin de déterminer si leurs terminaux POS POI sont affectés par les vulnérabilités du protocole SSL.

Pour les autres environnements (par ex., les terminaux de paiement virtuel, les serveurs de back-office, les ordinateurs d'utilisateurs, etc.) il est conseillé aux petits commerçants de préciser si le SSL/TLS initial est utilisé ou non, où il est utilisé, et de déterminer si une mise à niveau peut survenir immédiatement, ou si un impératif commercial justifie une mise à niveau tardive (mais pas au-delà du 30 juin 2018).

Quelques suggestions à considérer pour votre environnement :

- Vérifiez la version du navigateur Web utilisée par vos systèmes : les anciennes versions utilisent le SSL/TLS initial, et vous devrez peut-être opter pour un navigateur plus récent.
- Vérifiez les configurations de votre pare-feu pour voir si le SSL peut être bloqué.
- Assurez-vous que tous les correctifs de vos systèmes et de vos applications sont à jour.
- Vérifiez et contrôlez les systèmes afin d'identifier toute activité suspicieuse pouvant trahir un problème de sécurité.

En outre, lorsque vous planifiez une migration vers une alternative sécurisée, vous devez suivre un plan d’atténuation des risques et de migration.

Que doivent faire les commerçants dotés de terminaux POI prenant en charge le SSL/TLS initial ?

Le POI peut continuer avec le SSL/TLS initial si la preuve est avancée que le POI n’a pas de failles actuellement connues. Cependant, le SSL est une technologie désuète, qui peut encore faire l’objet d’autres vulnérabilités en matière de sécurité à l’avenir. Il est donc vivement recommandé de mettre à niveau les environnements POI vers le protocole TLS v1.1 ou une version supérieure dès que possible. Il est

fortement conseillé aux nouvelles implémentations de POI de prendre en charge et d'utiliser le protocole TLS v1.2, ou une version supérieure. Si le SSL/TLS initial n'est pas requis dans l'environnement, le recours et le repli relatifs à ces versions doivent être désactivés.

Lorsqu'ils évaluent les implémentations de terminaux POI utilisant le SSL/TLS initial, les évaluateurs doivent consulter les documents de soutien (par exemple, les documents fournis par le fournisseur de POI, les informations sur la configuration du système/du réseau, etc.) pour déterminer si l'implémentation est vulnérable aux failles connues.

Si l'environnement POS POI a des failles connues, envisager une migration vers un autre protocole sécurisé immédiatement.

Remarque : le recours autorisé aux POS POI sans failles actuellement connues repose sur des risques actuels et connus. Si de nouvelles failles sont introduites et que les environnements POI ne sont pas protégés, une mise à niveau est indispensable.

Pourquoi les environnements POS POI sont-ils moins vulnérables ?

La norme PCI DSS permet aux appareils des points d'interaction (POI) des points de vente (POS) et à leurs points de terminaison de continuer à utiliser le SSL et le TLS initial. En effet, les vulnérabilités connues au moment de la publication sont généralement plus difficiles à exploiter dans ces environnements.

Par exemple : certaines vulnérabilités actuelles du protocole SSL sont exploitées par un pirate qui intercepte une communication entre un client et un serveur pour manipuler les messages adressés au client. Le but du pirate est d'amener ce client à envoyer des informations supplémentaires, que le pirate utilisera pour compromettre la session. Les appareils des POS POI dotés des caractéristiques suivantes sont généralement plus résistants à ce type de vulnérabilité :

- L'appareil ne prend pas en charge les connexions multiples côté client (ce qui favorise la vulnérabilité POODLE).
- Le protocole de paiement adhère à la norme ISO 20022 (schéma universel de messages pour l'industrie financière), à la norme ISO 8583-1:2003 (messages initiés par cartes de transaction financière - spécifications d'échange de messages), ou à une norme équivalente limitant le nombre de données pouvant être exposées à des « attaques par rejeu ».
- L'appareil n'utilise ni logiciel de navigateur Web, ni JavaScript, ni cookie de session relatif à la sécurité.

Remarque : ces caractéristiques ne sont fournies qu'à titre d'exemple. Chaque implémentation devra être évaluée de manière indépendante afin de déterminer à quel point elle est sujette aux vulnérabilités.

Il importe aussi de se rappeler que les failles continuent d'évoluer, et que les organisations doivent se tenir prêtes à répondre aux nouvelles menaces. Toutes les organisations utilisant le SSL et/ou le TLS initial doivent se préparer à passer à un protocole à cryptographie robuste dès que possible.

Toute utilisation provisoire du protocole SSL ou TLS initial dans des environnements POS POI doit être accompagnée des correctifs à jour, et seules les extensions nécessaires doivent être activées.

Qu'est-ce que cela signifie pour les services de traitement de paiement prenant en charge les environnements POI ?

Des entités de tous types sont concernées par le problème du protocole SSL/TLS initial, y compris les services de traitement de paiement, les passerelles de paiement, et les autres entités proposant des services de traitement des transactions. Ces entités devront évaluer leur utilisation du SSL/TLS initial et planifier des migrations de la même manière que les autres entités.

Les entités proposant des services de traitement de paiement avec des points de terminaison de POI devront s'assurer que les communications POI ne sont pas vulnérables (comme indiqué dans la partie « Pourquoi les environnements POS POI sont-ils moins vulnérables ? », ci-dessus) si elles envisagent de continuer à utiliser le SSL/TLS initial.

Si une entité proposant des services de traitement de paiement prend en charge plusieurs canaux de paiement (par exemple, des transactions de commerce électronique et des POI), sur un même point de terminaison, elle devra s'assurer que tous les canaux vulnérables migrent vers une alternative sécurisée pour le 30 juin 2018. Si l'environnement POI est considéré comme non sujet aux vulnérabilités, l'entité pourra considérer les options suivantes :

- Migrer les canaux POI vers une alternative sécurisée pour que les transactions de commerce électronique et POI puissent continuer à utiliser le même point de terminaison.
- Si les canaux POI ne sont pas migrés, différent(e)s points de terminaison/interfaces peuvent être utilisé(e)s pour séparer le trafic POI qui utilise le SSL/TLS initial du trafic issu du commerce électronique ayant migré vers une alternative sécurisée.

Qu'en est-il des environnements de commerce électronique ?

En raison de la nature même des environnements basés sur le Web, les implémentations de commerce électronique, plus vulnérables, sont immédiatement exposées au risque des vulnérabilités connues des protocoles SSL et TLS initial.

C'est pour cette raison que les nouveaux sites Web de commerce électronique ne doivent pas utiliser ou prendre en charge le protocole SSL/TLS initial.

Les environnements de commerce électronique devant prendre en charge les clients utilisant le SSL/TLS initial doivent commencer à migrer dès que possible, et toutes les migrations doivent être effectuées pour le 30 juin 2018 au plus tard. Lorsqu'une migration ne peut avoir lieu immédiatement, une justification doit être documentée dans le cadre du plan d'atténuation des risques et de migration.

Tant que la migration n'est pas complète, il est conseillé de garder le moins de serveurs prenant en charge le SSL/TLS initial que possible. En diminuant le nombre de systèmes vulnérables, vous diminuez le risque de failles potentielles, et vous contribuez à rationaliser les contrôles d'atténuation des risques, comme le contrôle amélioré du trafic suspicieux.

Nous encourageons également les commerçants électroniques à conseiller à leurs clients de mettre à niveau leurs navigateurs Web pour qu'ils prennent en charge des protocoles sécurisés.

Comment lancer le processus de migration ?

Voici quelques suggestions pour aider les entités à planifier leur migration vers une alternative sécurisée :

1. Identifier les composants de système et les flux de données se basant sur et/ou prenant en charge les protocoles vulnérables.
2. Pour chaque composant de système ou flux de données, identifier la nécessité commerciale et/ou technique de l'utilisation d'un protocole vulnérable.
3. Supprimer ou désactiver immédiatement toutes les instances de protocoles vulnérables ne répondant pas à une nécessité commerciale ou technique.
4. Identifier des technologies pour remplacer les protocoles vulnérables et documenter les configurations sécurisées à implémenter.
5. Documenter un plan de migration reprenant les étapes et les échéances des mises à jour.
6. Implémenter des contrôles d'atténuation des risques pour contribuer à réduire les failles connues, jusqu'à ce que les protocoles vulnérables soient supprimés de l'environnement.
7. Effectuer des migrations et suivre les procédures de contrôle du changement afin de s'assurer que les mises à jour du système sont testées et autorisées.
8. Mettre à jour les normes de configuration du système dès complétion des migrations vers de nouveaux protocoles.

Les protocoles SSL/TLS initial peuvent-ils rester dans un environnement s'ils ne sont pas utilisés comme contrôle de sécurité ?

Oui, ces protocoles peuvent être utilisés sur un système tant que le SSL/TLS initial n'est pas utilisé comme contrôle de sécurité.

En outre, toutes les vulnérabilités des protocoles SSL/TLS obtenant un score CVSS de 4 ou plus lors d'un scan ASV, ou obtenant un résultat « élevé » lors d'un scan de vulnérabilité interne à une entité, doivent être résolues dans les délais impartis (de manière trimestrielle pour les scans ASV) afin de respecter l'exigence 11.2 de la norme PCI DSS. Observez les processus de gestion des vulnérabilités pour documenter la façon dont les vulnérabilités des protocoles SSL/TLS sont résolues, par exemple, là où ils sont utilisés uniquement pour les communications POI non vulnérables aux failles, ou là où ils sont présents mais pas utilisés comme contrôle de sécurité (par ex., là où ils ne sont pas utilisés pour protéger la confidentialité des communications).

Les dates de migration s'appliquent-elles si aucun incident de sécurité concernant les données du titulaire ne survient suite à l'utilisation des protocoles SSL/TLS initial ?

Oui, la date de migration depuis les protocoles SSL/TLS initial n'est pas affectée par le nombre d'incidents de sécurité concernant une carte de paiement pouvant ou non survenir à l'avenir. Les exigences de la norme PCI DSS sont conçues pour contribuer à éviter les incidents de sécurité concernant des données de titulaire grâce à une approche de défense profonde. Attendre que des failles potentielles concernant les données soient rendues publiques avant de prendre des mesures pour sécuriser vos propres données n'est pas une approche efficace de la sécurité, et n'est pas soutenue par la norme PCI DSS.

Dans quelle mesure la présence d'un protocole SSL influence-t-elle les résultats d'un scan ASV ?

Les protocoles SSL v3.0 et TLS initial contiennent un certain nombre de vulnérabilités, dont quelques-unes obtiennent actuellement un score de 4,3 dans le CVSS (système commun de notation des vulnérabilités). Le CVSS est défini par la NVD (base de données nationale des vulnérabilités) ; c'est le système de notation que les ASV doivent utiliser. Toute vulnérabilité à risque moyen ou élevé (c'est-à-dire les vulnérabilités obtenant un score CVSS de 4,0 ou plus) doit être corrigée, et les systèmes doivent être scannés à nouveau suite aux corrections afin de constater que le problème a bien été résolu.

Toutefois, comme il n'existe pas de manière connue de remédier à certaines de ces vulnérabilités, la mesure d'atténuation recommandée consiste à migrer vers une alternative sécurisée dès que possible. Les entités capables de migrer immédiatement vers une alternative sécurisée doivent travailler avec leur ASV pour documenter leur scénario particulier comme suit :

- *Avant le 30 juin 2018 :* les entités qui n'ont pas complété leur migration doivent fournir à leur ASV la confirmation documentée qu'ils ont implémenté un plan d'atténuation des risques et de migration, et qu'ils œuvrent à réaliser leur migration pour la date requise. Un reçu de cette confirmation doit être documenté par l'ASV comme une exception sous « Exceptions, faux positifs ou contrôles compensatoires » dans son résumé de rapport de scan, et l'ASV peut attribuer une note de « réussite » à ce composant de scan ou à cet hôte, si ce dernier respecte toutes les exigences de scan applicables.
- *Après le 30 juin 2018 :* les entités qui n'ont pas complètement migré depuis les protocoles SSL/TLS initial devront faire suivre le processus de réponse aux vulnérabilités par les contrôles compensatoires afin de s'assurer que le système affecté n'est pas sujet à des vulnérabilités particulières. Par exemple, lorsqu'un protocole SSL/TLS initial existe, mais n'est pas utilisé comme contrôle de sécurité (par ex., lorsqu'il n'est pas utilisé pour protéger la confidentialité des communications).

Les entités dotées de terminaux POS POI et/ou de points de terminaison vérifiés comme non sujets aux vulnérabilités spécifiques peuvent être éligibles pour une diminution de leur note NVD pour ces systèmes. Dans ce scénario, l'ASV doit fournir, outre tous les autres éléments de rapport requis, les informations suivantes en accord avec le guide de programme ASV :

- La note NVD de la vulnérabilité
- La note de la vulnérabilité de l'ASV
- La raison pour laquelle l'ASV n'est pas d'accord avec la note NVD

Par exemple, l'ASV peut déterminer qu'une vulnérabilité spécifique est plus difficile à exploiter dans un environnement POS POI particulier que ce qui a été défini par le système de notation NVD général. Dans ce cas, l'ASV peut reclasser cet élément du système de notation pour la vulnérabilité spécifique et pour les systèmes concernés.

Lorsqu'il effectue des réglages de ce type, l'ASV doit tenir compte de l'environnement, des systèmes et des contrôles uniques du client, et ne pas faire de réglages basés sur des suppositions ou des tendances générales. Le client du scan doit travailler avec son ASV pour expliquer son environnement ; autrement, l'ASV sera incapable de déterminer si la modification d'une note CVSS est appropriée.

Les ASV doivent faire preuve de diligence et d'attention lorsqu'ils font ces concessions, et ils doivent s'assurer que des éléments suffisants justifient une modification de la note CVSS. Toutes ces modifications doivent respecter les processus définis dans le guide de programme ASV.

Tous les rapports de scan ASV doivent être complétés en accord avec les processus du guide de programme ASV.

Cela signifie-t-il que les entités dotées d'un plan d'atténuation des risques et de migration n'ont pas de vulnérabilités au niveau des correctifs dans leur protocole SSL/TLS initial ?

Non, les dates cibles de la migration ne sont pas une excuse pour repousser les vulnérabilités de correctifs. De nouvelles menaces et de nouveaux risques continuent à être gérés selon les exigences de la norme PCI DSS applicables (6.1, 6.2 et 11.2, notamment), et les entités doivent résoudre les vulnérabilités dès qu'une mise à jour de sécurité ou un correctif est publié.

Quel est l'impact pour les services prenant en charge des protocoles sécurisés (par ex., TLS v1.2) ainsi que des protocoles non sécurisés (par ex., SSL/TLS initial) ?

Bon nombre de prestataires de services (par exemple, les fournisseurs d'hébergement partagé) proposent des plates-formes et des services à une large base de clients, pouvant inclure des entités obligées de respecter certaines exigences de la norme PCI DSS, et d'autres entités non soumises à ces obligations. Les prestataires de services prenant en charge le CDE d'un client peuvent soit démontrer qu'ils respectent les exigences applicables au nom du client, soit proposer des options de service respectant les exigences de la norme PCI DSS que leurs clients pourront utiliser. Le prestataire de services doit indiquer clairement à ses clients quels protocoles de sécurité il propose, comment configurer les différentes options, ainsi que les conséquences de l'utilisation des configurations considérées comme non sécurisées.

Par exemple, un fournisseur d'hébergement Web peut proposer aux commerçants une plateforme Web hébergée prenant en charge TLS v1.2, mais aussi des protocoles plus faibles. Pour soutenir son client dans son respect de la norme PCI DSS, le fournisseur d'hébergement doit fournir des instructions claires au client pour qu'il configure son utilisation du service de manière à n'utiliser le protocole TLS v1.2 que sans possibilité de repli vers le protocole SSL ou TLS initial. Du côté du client, un commerçant utilisant cette plateforme dans le cadre de son implémentation des normes PCI DSS devra s'assurer que les options de configuration qu'il utilise incluent l'utilisation du protocole TLS v1.2, sans possibilité de repli vers le protocole SSL/TLS initial.

La présence de protocoles plus faibles dans un environnement à hébergement mixte peut déclencher une faille du scan ASV. Si cela se produit, le prestataire de services et l'ASV devront suivre le processus des « Exceptions, faux positifs ou contrôles compensatoires » pour documenter la façon dont le risque a été géré (par exemple, en confirmant que le protocole SSL/TLS initial n'est pas utilisé comme contrôle de sécurité par le prestataire de services, et que des options de configuration sécurisée ne permettant pas de repli vers des protocoles plus faibles sont proposées au client). L'ASV pourra alors attribuer une note de « réussite » à ce composant de scan ou à cet hôte, si ce dernier respecte toutes les exigences de scan applicables.