SUPLEMENTO INFORMATIVO

Migrar de SSL y TLS temprana

Versión 1.1
Fecha: Abril de 2016
Autor: PCI Security Standards Council

Resumen ejecutivo

El momento para migrar es ahora.

Por más de 20 años, Secure Sockets Layer (SSL) ha estado en el mercado como uno de los protocolos de cifrado más utilizados que alguna vez se haya lanzado, y sigue siendo de uso generalizado hoy en día, a pesar de diversas vulnerabilidades de seguridad expuestas en el protocolo.

SSL v3.0 fue reemplazada en 1999 por TLS v1.0, que desde entonces ha sido sustituida por TLS v1.1 y v1.2. Hasta la fecha, SSL y TLS temprana ya no cumplen con las normas mínimas de seguridad debido a las vulnerabilidades de seguridad en el protocolo, para las que no hay reparación. Es fundamental que las entidades se actualicen a una alternativa segura lo antes posible, y que desactiven todo repliegue a SSL y TLS temprana.

SSL/TLS temprana se eliminó como ejemplo de criptografía sólida en PCI DSS v3.1 (Abril de 2015).

¿Cuál es el riesgo?

SSL/TLS cifra un canal entre dos extremos (por ejemplo, entre un navegador web y el servidor web) para proporcionar privacidad y confiabilidad de los datos transmitidos por el canal de comunicaciones. Desde el lanzamiento de la versión 3.0 de SSL, se han identificado diversas vulnerabilidades, más recientemente, a finales de 2014 cuando los investigadores publicaron detalles sobre una vulnerabilidad de seguridad (CVE-2014-3566) que puede permitir a los atacantes extraer datos de las conexiones seguras. Más comúnmente conocida como POODLE (Padding Oracle On Downgraded Legacy Encryption), esta vulnerabilidad es un ataque intermedio donde es posible descifrar un mensaje cifrado que está asegurado por SSL v3.0.

El protocolo SSL (todas las versiones) no se puede reparar; no existen métodos conocidos para remediar las vulnerabilidades como POODLE. SSL y TLS temprana ya no cumplen con las necesidades de seguridad de las entidades que implementan criptografía sólida para proteger los datos de pago en canales de comunicación públicos o no confiables. Además, los navegadores web modernos han comenzado a prohibir las conexiones SSL, lo que evita que los usuarios de estos navegadores accedan a servidores web que no han migrado a un protocolo más moderno.

¿Cómo debo responder?

La mejor respuesta es deshabilitar SSL en su totalidad y migrar a un protocolo de cifrado más moderno, que en el momento de la publicación es un mínimo de TLS v1.1, aunque se recomienda enfáticamente que las entidades consideren TLS v1.2. Tenga en cuenta que no todas las implementaciones de TLS v1.1 se consideran seguras - consulte NIST SP 800-52 rev. 1 para obtener orientación sobre las configuraciones seguras de TLS.

Qué significa esto para la PCI DSS

A partir de la PCI DSS v3.1, SSL y TLS temprana ya no son ejemplos de criptografía sólida o de protocolos seguros. Los requisitos de la PCI DSS directamente afectados son:

Requisito 2.2.3	Implementar funciones de seguridad adicionales para los servicios, protocolos o daemons requeridos que no se consideren seguros.
Requisito 2.3	Cifre todo el acceso administrativo que no sea de consola utilizando una criptografía sólida.
Requisito 4.1	Utilice criptografía y protocolos de seguridad sólidos para salvaguardar los datos confidenciales de los titulares de las tarjetas durante su transmisión a través de redes públicas abiertas.

SSL y TLS temprana no deberán utilizarse como un control de seguridad para cumplir estos requisitos. Para apoyar a las entidades que trabajan para migrar de SSL/TLS temprana, se incluyen las siguientes disposiciones:

- Las nuevas implementaciones no deben utilizar SSL o TLS temprana como control de seguridad (la orientación sobre las implementaciones nuevas y existentes se proporciona en la siguiente sección)
- Todos los proveedores de servicios deben ofrecer una oferta de servicios de TLS segura al 30 de junio de **2016**.
- Después del 30 de junio de **2018**, todas las entidades deberán haber dejado de usar la SSL/TLS temprana como un control de seguridad, y usar solo las versiones seguras del protocolo (se describe una asignación para determinados terminales POS POI en la última viñeta a continuación).
- Antes del 30 de junio de 2018, las implementaciones que utilizan SSL y/o TLS temprana deben tener un Plan de migración y de mitigación de riesgo formal implementados.
- Las terminales POS POI (y los puntos de terminación SSL/TLS a los que se conectan) que pueden ser verificadas como no susceptibles a cualquier ataque conocido para SSL y TLS temprana, pueden seguir utilizando estos como un control de seguridad después del 30 de junio de 2018.

Si se usa SSL/TLS temprana, se aplican los requisitos de la PCI DSS Anexo A2 "*Requisitos adicionales de la PCI DSS para las entidades que utilizan SSL/TLS temprana*".

Entender implementaciones "nuevas" y "existentes"

Las implementaciones se consideran "implementaciones nuevas" cuando no hay dependencia existente del uso de los protocolos vulnerables. Los escenarios de ejemplo que podrían considerarse implementaciones "nuevas" incluyen:

- La instalación de un sistema en un entorno que actualmente solo utiliza protocolos seguros
- La instalación de una aplicación en un sistema que actualmente utiliza solo protocolos seguros
- La construcción de un nuevo sistema o red para comunicarse con otros sistemas/redes que soportan protocolos seguros

Si una nueva implementación no necesita soportar un uso preexistente de un protocolo vulnerable, se debe implementar solo con protocolos seguros y criptografía sólida, y se debe configurar para no permitir el repliegue al protocolo vulnerable.

Nota: *Las nuevas implementaciones de comercio electrónico no deben considerar a los navegadores web de los consumidores como infraestructura preexistente que necesita soporte.*

Por el contrario, las implementaciones "existentes" son aquellas en las que hay una dependencia o el uso preexistente de un protocolo(s) vulnerable. Los escenarios de ejemplo que podrían considerarse implementaciones "existentes" incluyen:

- La instalación de un sistema en un entorno que actualmente solo utiliza y/o tiene una necesidad de dar soporte a protocolos vulnerables
- La instalación de una aplicación en un sistema que actualmente utiliza y/o tiene una necesidad de dar soporte a protocolos vulnerables
- La construcción de un nuevo sistema o red para comunicarse con otros sistemas/redes que actualmente utilizan protocolos vulnerables

Se recomienda que las implementaciones existentes se actualicen de inmediato, ya que el uso continuo de SSL/TLS temprana podría poner en riesgo al entorno.

Preparación de un Plan de migración y Mitigación de riesgos

El Plan de Mitigación y Migración de riesgos es un documento preparado por la entidad que detalla sus planes para migrar a un protocolo seguro, y también describe los controles que la entidad ha implementado para reducir el riesgo asociado con SSL/TLS temprana hasta que finalice la migración. Se tendrá que proporcionar el Plan de migración y Mitigación de riesgos al evaluador como parte del proceso de evaluación de la PCI DSS.

A continuación se proporciona orientación y ejemplos de información que se documentarán en el Plan de migración y Mitigación de riesgos:

- Descripción de cómo se utilizan los protocolos vulnerables, incluido;
    - El tipo de entorno en el que se utilizan los protocolos, por ejemplo, el tipo de canal y las funciones de pago para los que utilizan los protocolos
    - El tipo de datos que se transmite, por ejemplo, los elementos de datos de cuentas de las tarjetas de pago, las conexiones administrativas, etc.
    - El número y los tipos de sistemas que utilizan y/o soportan los protocolos, por ejemplo, las terminales POI POS, los conmutadores de pago, etc.
- Resultados de la evaluación de riesgos y controles de reducción de riesgos implementados:
    - Las entidades deberán haber evaluado y documentado el riesgo para el entorno e implementado controles de reducción de riesgos para ayudar a mitigar el riesgo hasta que se pueda eliminar por completo los protocolos vulnerables.
- Descripción de los procesos que se implementan para supervisar las nuevas vulnerabilidades asociadas con los protocolos vulnerables:
    - Las entidades necesitan ser proactivas y estar informadas acerca de las vulnerabilidades. A medida que se publican las nuevas vulnerabilidades, la entidad tiene que evaluar el riesgo que suponen para el entorno y determinar si los controles adicionales de reducción de riesgo necesitan implementarse hasta que se complete la migración.
- Descripción de los procesos de control de cambios que se implementan para garantizar que SSL/TLS temprana no se implementa en los nuevos entornos:
    - Si una entidad no utiliza o necesita apoyar los protocolos vulnerables actualmente, no hay razón por la que deban introducir dichos protocolos a su entorno. Los procesos de control de cambios incluyen a la evaluación del impacto del cambio para confirmar que el cambio no introduce una nueva debilidad en la seguridad del entorno.
- El resumen del plan de proyecto de migración incluye la fecha de finalización de la migración objetivo no más tarde del 30 de junio de 2018:
    - La documentación de planificación de la migración incluye la identificación de los sistemas/entornos que se están migrando y cuándo, así como una fecha prevista para la que se completará la migración general. La fecha prevista para la migración general debe ser el, o antes del 30 de junio de 2018.

Preguntas frecuentes

¿Qué son los controles de mitigación del riesgo?

Para los entornos que utilizan actualmente protocolos vulnerables, la implementación y el uso continuo de los controles de mitigación de riesgos ayuda a proteger el entorno vulnerable hasta que se complete la migración hacia una alternativa segura.

Algunos controles que pueden ayudar con la reducción del riesgo incluyen, pero no se limitan a:

- La reducción al mínimo de la superficie de ataque tanto como sea posible, al consolidar las funciones que utilizan protocolos vulnerables en menos sistemas, y reducir el número de sistemas que soportan los protocolos.
- La eliminación o desactivación del uso de navegadores web, JavaScript y las cookies de sesión que afectan a la seguridad cuando no se necesitan.
- La restricción del número de comunicaciones que utilizan los protocolos vulnerables al detectar y bloquear las solicitudes para regresar a una versión de protocolo menor.
- La restricción del uso de los protocolos vulnerables para entidades específicas; por ejemplo, al configurar los firewalls para permitir SSL/TLS temprana solo para las direcciones IP conocidas (como los socios comerciales que requieren el uso de los protocolos), y bloquear dicho tráfico para todas las demás direcciones IP.
- Mejorar las capacidades de detección/prevención al ampliar la cobertura de los sistemas de protección contra la intrusión, actualizar las firmas, y bloquear la actividad de red que indica un comportamiento malicioso.
- Supervisar de manera activa la actividad sospechosa, por ejemplo, identificar aumentos inusuales en las solicitudes para el repliegue a protocolos vulnerables, y responder adecuadamente.

Además, las entidades deberán garantizar que todos los requisitos aplicables de la PCI DSS también están implementados, incluido:

- Mantener informado de manera proactiva acerca de las vulnerabilidades nuevas; por ejemplo, suscribirse a los servicios de notificación de vulnerabilidad y a los sitios de soporte de proveedores para recibir actualizaciones de las vulnerabilidades nuevas a medida que surgen.
- Aplicar las recomendaciones del proveedor para configurar sus tecnologías de manera segura.

¿Cuáles son algunas de las opciones de migración?

Los ejemplos de medidas criptográficas adicionales que se puedan implementar y utilizar como control de seguridad para reemplazar a SSL/TLS temprana pueden incluir:

- Actualizar a una versión actual y segura de TLS que se implementa de manera segura y se configura para no aceptar el repliegue a la SSL o TLS temprana.
- Cifrar los datos con la criptografía sólida antes de enviarlos a través de SSL/TLS temprana (por ejemplo, utilizar el cifrado de nivel de campo o de nivel de aplicación para cifrar los datos antes de la transmisión)
- Primero configurar una sesión cifrada fuertemente (por ejemplo, el túnel IPsec), luego enviar los datos a través de SSL dentro del túnel seguro

Además, el uso de la autenticación de dos factores se puede combinar con los controles anteriores para proporcionar una certeza de autenticación.

La elección de un control criptográfico alternativo dependerá de las necesidades técnicas y comerciales para un entorno en particular.

¿Qué sucede con los entornos comerciantes pequeños?

Todos los tipos de entidades se ven afectadas por los problemas con SSL/TLS temprana, incluidos los comerciantes pequeños. Es fundamental que los comerciantes pequeños tomen las medidas necesarias para eliminar SSL/TLS temprana del entorno de sus datos del titular de la tarjeta para garantizar que los datos de su cliente estén seguros.

Para el entorno POI, se recomienda que los pequeños comerciantes se contacten con su proveedor de terminal y/o adquirente (banco del comerciante) para determinar si sus terminales POI POS se ven afectadas por las vulnerabilidades de SSL.

Para otros entornos, por ejemplo, las terminales de pago virtuales, los servidores de back-office, etc. las computadoras de los usuarios etc., los pequeños comerciantes deberán validar si se utiliza SSL/TLS temprana y dónde se implementa, y luego determinar si se puede producir una actualización de inmediato, o si existe una justificación comercial para una actualización retrasada (que no supere el 30 de junio de 2018).

Las sugerencias para lo que se debe tener en cuenta en su entorno incluyen:

- Comprobar la versión del navegador web que utilizan sus sistemas, las versiones más antiguas utilizarán SSL/TLS temprana y es posible que tenga que actualizar a un navegador más reciente
- Comprobar las configuraciones del Firewall para determinar si se puede bloquear SSL
- Comprobar que todas las aplicaciones y los parches del sistema estén actualizados
- Comprobar y supervisar los sistemas para identificar actividades sospechosas que puedan indicar un problema de seguridad

Además, al planificar su migración a una alternativa segura, debe completar un Plan de migración y Mitigación de riesgos.

¿Qué deberán hacer los comerciantes con las terminales POI que soportan SSL/TLS temprana?

Los POI puede seguir usando SSL/TLS temprana, cuando se puede mostrar que el POI no es susceptible al ataque conocido actualmente. Sin embargo, SSL es una tecnología obsoleta y puede estar sujeta a las vulnerabilidades de seguridad adicionales en el futuro; por lo tanto, se recomienda encarecidamente que los entornos de POI se actualicen a TLS v1.1 o superior lo antes posible. Las nuevas implementaciones de los POI deberán considerar seriamente el soporte y el uso de TLS 1.2 o superior. Si SSL/TLS temprana no es necesaria en el entorno, se debe desactivar el uso y el repliegue de estas versiones.

Al revisar las implementaciones de las terminales POI que utilizan SSL/TLS temprana, los evaluadores deberán revisar la documentación de apoyo (por ejemplo, la documentación proporcionada por el proveedor de POI, los detalles de configuración del sistema/red, etc.) para determinar si la implementación es susceptible a ataques conocidos.

Si el entorno de POS POI es susceptible a ataques conocidos, entonces debe comenzar la planificación de la migración a una alternativa segura de inmediato.

Nota: La provisión para POS POI que actualmente no son susceptibles al ataque se basa en los riesgos actuales, conocidos. Si se introducen nuevos ataques para los que los entornos de POI son susceptibles, tendrán que actualizarse los entornos de POI.

¿Por qué los entornos de POI POS son menos vulnerables?

La PCI DSS proporciona una asignación para SSL y TLS temprana para seguir siendo utilizada por los dispositivos de punto de interacción (POI) punto de venta (POS) y sus terminales. Esto se debe a que las vulnerabilidades conocidas en el momento de la publicación son generalmente más difíciles de atacar en estos entornos.

Por ejemplo: Algunas de las vulnerabilidades de SSL actuales son explotadas por un atacante que intercepta la comunicación cliente/servidor y manipula los mensajes para el cliente. El objetivo del atacante es engañar al cliente para que envíe datos adicionales que el atacante puede utilizar para poner en riesgo la sesión. Los dispositivos POI POS con las siguientes características son generalmente más resistentes a este tipo de vulnerabilidad:

- El dispositivo no soporta conexiones múltiples del lado del cliente (que facilita el ataque de POODLE).
- El protocolo de pago se adhiere a la norma ISO 20022 (Esquema universal de mensajes para el sector financiero)/ISO 8583-1: 2003 (Mensajes de transacciones financieras originados por tarjeta - Especificaciones de intercambio de mensajes), o a la norma equivalente que limita la cantidad de los datos expuestos en “ataques de respuesta”.
- El dispositivo no utiliza software de navegador web, JavaScript o cookies de sesión relacionadas con la seguridad.

Nota: Estas características están destinadas solo como ejemplo; cada implementación tendrá que ser evaluada de manera independiente para determinar el grado de susceptibilidad a las vulnerabilidades.

También es importante recordar que los ataques continúan evolucionando y las organizaciones deben estar preparadas para responder a las nuevas amenazas. Todas las organizaciones que utilizan SSL y/o TLS temprana deberán planificar actualizarse a un protocolo de criptografía sólida, lo antes posible.

Cualquier uso provisional de SSL/TLS temprana en entornos POI POS debe tener parches actualizados, y garantizar que solo se habiliten las extensiones necesarias.

¿Qué significa esto para los procesadores de pago que soportan los entornos POI?

Las entidades de todo tipo se ven afectadas por el problema de SSL/TLS temprana, incluidos los procesadores de pago, las puertas de enlace de pago, y otras entidades que prestan servicios de procesamiento de transacciones. Estas entidades tendrán que revisar su uso de SSL/TLS temprana y planificar las migraciones de la misma manera que otras entidades.

Las entidades de procesamiento de pago con terminales POI tendrán que verificar las comunicaciones POI que no son vulnerables (como se describe en la sección anterior “¿Por qué son menos vulnerables los entornos POI POS?”) si van a seguir utilizando SSL/TLS temprana.

Si una entidad de procesamiento de pagos soporta múltiples canales de pago, por ejemplo, las transacciones POI y de comercio electrónico, en la misma terminal, la entidad tendrá que asegurarse de que todos los canales vulnerables se migren a una alternativa segura antes del 30 de junio de 2018. Si el entorno de POI se considera como no susceptible a las vulnerabilidades, la entidad podría considerar las siguientes opciones:

- Migrar los canales de POI hacia una alternativa segura para que las transacciones de comercio electrónico y de POI puedan seguir utilizando la misma terminal.
- Si los canales POI no se están migrando, los puntos de terminación separados/interfaces pueden ser utilizados para separar el tráfico de POI que utiliza SSL/TLS temprana del tráfico de comercio electrónico que ha migrado hacia una alternativa segura.

¿Qué pasa con los entornos de comercio electrónico?

Debido a la naturaleza de los entornos basados en la web, las implementaciones de comercio electrónico tienen la mayor susceptibilidad y están, por lo tanto, en situación de riesgo inmediato de las vulnerabilidades conocidas en SSL/TLS temprana.

Debido a esto, los sitios web de comercio electrónico nuevos no deben utilizar o dar soporte a SSL/TLS temprana.

Los entornos de comercio electrónico que tienen una necesidad actual de dar soporte a los clientes que utilizan SSL/TLS temprana deben empezar a migrar lo antes posible, con todas las migraciones completas para el 30 de junio de 2018. Donde la migración no se pueda producir de inmediato, se debe documentar la justificación como parte del Plan de migración y Mitigación de riesgos.

Hasta que finalice la migración, se recomienda que el número de servidores que soportan SSL/TLS temprana se minimice a la menor cantidad posible. Reducir el número de sistemas vulnerables reduce la exposición potencial a los ataques, y también puede ayudar a simplificar los controles de mitigación de riesgo, como la supervisión mejorada del tráfico sospechoso.

También animamos a los comerciantes de comercio electrónico que sugieran a sus clientes actualizar los navegadores de Internet para soportar los protocolos seguros.

¿Por dónde empezar con el proceso de migración?

Aquí hay algunos pasos sugeridos para ayudar a las entidades a planificar su migración hacia una alternativa segura:

1. Identificar todos los componentes del sistema y los flujos de datos que confían y/o dan soporte a los protocolos vulnerables
2. Para cada componente del sistema o para el flujo de datos, identifique la necesidad comercial y/o técnica para utilizar el protocolo vulnerable
3. Elimine o deshabilite de inmediato todas las instancias de los protocolos vulnerables que no cuentan con una necesidad comercial o técnica de soporte
4. Identificar tecnologías para reemplazar los protocolos vulnerables y documentar las configuraciones seguras que se implementarán
5. Documentar un plan de proyecto de migración que describa los pasos y los plazos para las actualizaciones
6. Implementar controles de reducción de riesgos para ayudar a reducir la susceptibilidad a los ataques conocidos hasta que se eliminen los protocolos vulnerables del entorno
7. Realizar migraciones y seguir los procedimientos de control de cambios para garantizar que se prueban y autorizan las actualizaciones del sistema
8. Actualizar las normas de configuración del sistema a medida que se completan las migraciones a los nuevos protocolos

¿Puede SSL/TLS temprana permanecer en un entorno si no se utiliza como un control de seguridad?

Sí, estos protocolos pueden permanecer en uso en un sistema, siempre que SSL/TLS temprana no se utilicen como un control de seguridad.

Además, todas las vulnerabilidades de SSL/TLS que obtienen una puntuación de CVSS 4 o superior en una exploración de ASV, o que están clasificadas como “altas” en la exploración interna de vulnerabilidades de una entidad, deberán abordarse dentro del plazo establecido (por ejemplo, trimestral para las exploraciones de ASV) con el fin de satisfacer el Requisito 11.2. de la PCI DSS. Seguir los procesos de gestión de vulnerabilidad definidos para documentar cómo se abordan las vulnerabilidades de SSL/TLS, por ejemplo, donde solo se utiliza para comunicaciones de POI que no son susceptibles a los ataques, o en los que está presente pero que no se utiliza como un control de seguridad (por ejemplo, no se utiliza para proteger la confidencialidad de la comunicación).

¿Se aplican las fechas de migración si no hay riesgos para los datos del titular de la tarjeta que sean resultantes del uso de SSL/TLS temprana?

Sí, la fecha para la migración de SSL/TLS temprana no se ve afectada por el número de riesgos para los datos de las tarjetas de pago que puedan o no producirse en el futuro. Los requisitos de la PCI DSS tienen por objeto ayudar a prevenir los riesgos de los datos del titular de

la tarjeta mediante un enfoque de defensa en profundidad. Esperar que se publiquen las posibles violaciones de datos antes de tomar medidas para proteger sus propios datos no es un método eficaz para la seguridad, y no tiene soporte de la PCI DSS.

¿De qué manera la presencia de SSL afecta a los resultados de las exploraciones de ASV?

SSL v3.0 y TLS temprana contienen una serie de vulnerabilidades, algunas de las cuales dan lugar a una puntuación de 4,3 en el Sistema de puntuación de vulnerabilidad común (Common Vulnerability Scoring System, CVSS). El CVSS está definido por la Base de datos de vulnerabilidad nacional (National Vulnerability Database, NVD) y es el sistema de puntuación que se exige que el ASV utilice. Cualquier vulnerabilidad de riesgo medio o alto (es decir, las vulnerabilidades con un CVSS de 4,0 o superior) debe ser corregida y los sistemas afectados explorados nuevamente después de las correcciones para mostrar que el problema se ha resuelto.

Sin embargo, ya que no hay manera conocida para remediar algunas de estas vulnerabilidades, la mitigación recomendada es migrar hacia una alternativa segura lo antes posible. Las entidades que no pueden migrar de inmediato hacia una alternativa segura deberán trabajar con sus ASV para documentar su escenario en particular como sigue:

- *Antes del 30 de junio de 2018:* Las entidades que no han completado su migración, deberán proporcionar al ASV la confirmación documentada que han implementado un Plan de migración y Mitigación de riesgos y que están trabajando para completar su migración para la fecha requerida. La recepción de esta confirmación deberá ser documentada por el ASV como una excepción en “Exceptions, False Positives, or Compensating Controls” (Excepciones, falsos positivos o controles de compensación) en el Resumen ejecutivo del informe de exploración del ASV, y el ASV podrá emitir un resultado de ”Aprobado” para ese componente de exploración o host, si este cumple todos los requisitos aplicables de exploración.
- *Después del 30 de junio de 2018:* Las entidades que no han migrado completamente de SSL/TLS temprana tendrán que seguir el proceso de Abordar las vulnerabilidades con los Controles de compensación para verificar que el sistema afectado no es susceptible a las vulnerabilidades particulares. Por ejemplo, cuando SSL/TLS temprana está presente pero no se utiliza como un control de seguridad (por ejemplo, no se utiliza para proteger la confidencialidad de la comunicación).

Las entidades con terminales POI POS y/o puntos de terminación que se verifican como no susceptibles a las vulnerabilidades específicas, pueden ser elegibles para una reducción en la puntuación de la NVD para esos sistemas. En este escenario, el ASV debe proporcionar (además de todos los demás elementos de presentación de informes necesarios), la siguiente información de acuerdo con la Guía de programa del ASV:

- La calificación de la NVD de la vulnerabilidad
- La calificación del ASV de la vulnerabilidad
- Por qué el ASV no está de acuerdo con la calificación de la NVD

Por ejemplo, el ASV podría determinar que una vulnerabilidad específica tiene una dificultad mayor para atacar un entorno POI POS particular que la definida por el sistema general de puntuación de la NVD. El ASV puede entonces volver a clasificar este elemento del sistema de puntuación para la vulnerabilidad específica, para los sistemas en cuestión.

Al realizar ajustes de este tipo, el ASV debe considerar el entorno, los sistemas y los controles únicos del cliente, y no hacer dichos ajustes basados en las tendencias o suposiciones generales. El cliente de exploración deberá trabajar con su ASV para proporcionar una comprensión de su entorno; de lo contrario el ASV no podrá determinar si es apropiado cambiar una puntuación del CVSS.

Los ASV deben actuar con la diligencia debida y el cuidado debido cuando empleen dichas concesiones, y deben garantizar que existen pruebas suficientes para apoyar un cambio en la puntuación del CVSS. Todos estos cambios deben seguir el proceso definido en la Guía de programa del ASV.

Todos los informes de exploración del ASV deben completarse de acuerdo con los procesos de la Guía de programa del ASV.

¿Esto quiere decir que las entidades con un Plan de migración y Mitigación de riesgos no tienen que parchar las vulnerabilidades en SSL/TLS temprana?

No, las fechas de migración previstas no son una excusa para retrasar el parche de las vulnerabilidades. Las nuevas amenazas y riesgos deben seguir manejándose de conformidad con los requisitos aplicables de la PCI DSS, por ejemplo, 6.1, 6.2 y 11.2, y las entidades deben abordar las vulnerabilidades donde esté disponible una actualización, reparación o parche de seguridad.

¿Cuál es el impacto de los servicios que soportan los protocolos seguros (por ejemplo, TLS v1.2), así como los protocolos inseguros (por ejemplo, SSL/TLS temprana)?

Muchos proveedores de servicios (por ejemplo, los proveedores de hosting compartido) proporcionan plataformas y servicios para una amplia base de clientes, que puede incluir a las entidades que necesitan cumplir los requisitos de la PCI DSS, así como las entidades que no necesitan hacerlo. Los proveedores de servicios que apoyan el CDE de un cliente pueden demostrar que están cumpliendo los requisitos aplicables en nombre del cliente, o que están proporcionando opciones de servicios que cumplen los requisitos de la PCI DSS para que los utilicen sus clientes. El proveedor de servicios deberá comunicar claramente a sus clientes qué protocolos de seguridad se ofrecen, cómo configurar las diferentes opciones, y el impacto de usar las configuraciones que se consideran inseguras.

Por ejemplo, un proveedor de hosting de web puede ofrecer una plataforma web alojada para los comerciantes que soporta TLS v1.2 y que también soporta los protocolos más débiles. Para apoyar el cumplimiento de la PCI DSS de sus clientes, el proveedor de hosting debe proporcionar instrucciones claras para que el cliente configure su uso del servicio para utilizar solo TLS v1.2 sin repliegue a SSL/TLS temprana. Desde el lado del cliente, un comerciante que utiliza esta plataforma como parte de su implementación de la PCI DSS tendrá que garantizar que las opciones de configuración que están utilizando incluyen el uso de TLS v1.2 sin repliegue a SSL/TLS temprana.

La presencia de protocolos más débiles en un entorno de alojamiento mixto puede provocar una falla en la exploración del ASV. Cuando esto ocurre, el proveedor de servicios y el ASV deberán seguir el proceso “Excepciones, falsos positivos o controles de compensación” para documentar cómo se ha abordado el riesgo, por ejemplo, al confirmar que SSL/TLS temprana no se utilizan como un control de seguridad por parte del proveedor de servicios, y que se proporcionan las opciones de configuración seguras que no permiten el repliegue a los protocolos más débiles para el uso de los clientes. El ASV podrá entonces emitir un resultado de “Aprobado” para ese componente de exploración o host, si el host cumple todos los requisitos de exploración aplicables.