INFORMATION SUPPLEMENT

Migrating from SSL and Early TLS

Version 1.1
Date: April 2016
Author: PCI Security Standards Council

Executive Summary

The time to migrate is now.

For over 20 years Secure Sockets Layer (SSL) has been in the market as one of the most widely-used encryption protocols ever released, and remains in widespread use today despite various security vulnerabilities exposed in the protocol.

SSL v3.0 was superseded in 1999 by TLS v1.0, which has since been superseded by TLS v1.1 and v1.2. To date, SSL and early TLS no longer meet minimum security standards due to security vulnerabilities in the protocol for which there are no fixes. It is critically important that entities upgrade to a secure alternative as soon as possible, and disable any fallback to both SSL and early TLS.

SSL/early TLS was removed as an example of strong cryptography in PCI DSS v3.1 (April 2015).

What is the risk?

SSL/TLS encrypts a channel between two endpoints (for example, between a web browser and web server) to provide privacy and reliability of data transmitted over the communications channel. Since the release of SSL v3.0, several vulnerabilities have been identified, most recently in late 2014 when researchers published details on a security vulnerability (CVE-2014-3566) that may allow attackers to extract data from secure connections. More commonly referred to as POODLE (Padding Oracle On Downgraded Legacy Encryption), this vulnerability is a man-in-the-middle attack where it's possible to decrypt an encrypted message secured by SSL v3.0.

The SSL protocol (all versions) cannot be fixed; there are no known methods to remediate vulnerabilities such as POODLE. SSL and early TLS no longer meet the security needs of entities implementing strong cryptography to protect payment data over public or untrusted communications channels. Additionally, modern web browsers have begun prohibiting SSL connections, preventing users of these browsers from accessing web servers that have not migrated to a more modern protocol.

How should I respond?

The best response is to disable SSL entirely and migrate to a more modern encryption protocol, which at the time of publication is a minimum of TLS v1.1, although entities are strongly encouraged to consider TLS v1.2. Note that not all implementations of TLS v1.1 are considered secure – refer to NIST SP 800-52 rev 1 for guidance on secure TLS configurations.

What this means for PCI DSS

As of PCI DSS v3.1, SSL and early TLS are no longer examples of strong cryptography or secure protocols. The PCI DSS requirements directly affected are:

Requirement 2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.
Requirement 2.3	Encrypt all non-console administrative access using strong cryptography.
Requirement 4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.

SSL and early TLS should not be used as a security control to meet these requirements. To support entities working to migrate away from SSL/early TLS, the following provisions are included:

- New implementations must not use SSL or early TLS as a security control (guidance on new and existing implementations is provided in the next section)
- All service providers must provide a secure TLS service offering by June 30, **2016**

- After June 30, **2018**, all entities must have stopped use of SSL/early TLS as a security control, and use only secure versions of the protocol (an allowance for certain POS POI terminals is described in the last bullet, below).
- Prior to June 30, 2018, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.
- POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS, may continue using these as a security control after 30th June, 2018.

If SSL/early TLS is used, the requirements in PCI DSS Appendix A2 *"Additional PCI DSS Requirements for Entities using SSL/Early TLS"* apply.

Understanding "new" and "existing" implementations

Implementations are considered "new implementations" when there is no existing dependency on the use of the vulnerable protocols. Example scenarios that would be considered "new" implementations include:

- Installing a system into an environment that currently uses only secure protocols
- Installing an application onto a system that currently uses only secure protocols
- Building a new system or network to communicate with other systems/networks that support secure protocols

If a new implementation does not need to support a pre-existing use of a vulnerable protocol, it must be implemented with only secure protocols and strong cryptography, and be configured to not allow fallback to the vulnerable protocol.

Note: *New e-commerce implementations must not consider consumer web browsers as pre-existing infrastructure that needs to be supported.*

Conversely, "existing" implementations are those where there is a pre-existing reliance or use of a vulnerable protocol(s). Example scenarios that would be considered "existing" implementations include:

- Installing a system into an environment that currently uses and/or has a need to support vulnerable protocols
- Installing an application onto a system that currently uses and/or has a need to support vulnerable protocols
- Building a new system or network to communicate with other systems/networks that currently use vulnerable protocols

It is recommended that existing implementations be upgraded immediately, as continued use of SSL/early TLS could put the environment at risk.

Preparing a Risk Mitigation and Migration Plan

The Risk Mitigation and Migration Plan is a document prepared by the entity that details their plans for migrating to a secure protocol, and also describes controls the entity has in place to reduce the risk associated with SSL/early TLS until the migration is complete. The Risk Mitigation and Migration Plan will need to be provided to the assessor as part of the PCI DSS assessment process.

The following provides guidance and examples of information to be documented in the Risk Mitigation and Migration Plan:

- Description of how vulnerable protocols are used, including;
  - The type of environment where the protocols are used – e.g. the type of payment channel and functions for which the protocols are used
  - The type of data being transmitted – e.g. elements of payment card account data, administrative connections etc.
  - Number and types of systems using and/or supporting the protocols – e.g. POS POI terminals, payment switches, etc.
- Risk assessment results and risk reduction controls in place:
  - Entities should have evaluated and documented the risk to their environment and have implemented risk reduction controls to help mitigate the risk until the vulnerable protocols can be completely removed.
- Description of processes that are implemented to monitor for new vulnerabilities associated with vulnerable protocols:
  - Entities need to be proactive and stay informed about new vulnerabilities. As new vulnerabilities are published, the entity needs to evaluate the risk they pose to their environment and determine if additional risk reduction controls need to be implemented until the migration is complete.
- Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments:

  - If an entity does not currently use or need to support vulnerable protocols, there is no reason why they should introduce such protocols to their environment. Change controls processes include evaluating the impact of the change to confirm the change does not introduce a new security weakness into the environment.
- Overview of migration project plan including target migration completion date no later than 30th June 2018:
  - Migration planning documentation includes identifying which systems/environments are being migrated and when, as well as a target date by which the overall migration will be completed. The target date for the overall migration must be on or before 30th June 2018.

Frequently Asked Questions

What are risk-mitigation controls?

For environments currently using vulnerable protocols, the implementation and continued use of risk-mitigation controls helps protect the vulnerable environment until migration to a secure alternative is complete.

Some controls that may help with risk reduction include, but are not limited to:

- Minimizing the attack surface as much as possible, by consolidating functions that use vulnerable protocols onto fewer systems, and reducing the number of systems supporting the protocols.
- Removing or disabling use of web browsers, JavaScript, and security-impacting session cookies where they are not needed.
- Restricting the number of communications using the vulnerable protocols by detecting and blocking requests to downgrade to a lesser protocol version.
- Restricting use of the vulnerable protocols to specific entities; for example, by configuring firewalls to permit SSL/early TLS only to known IP addresses (such as business partners requiring use of the protocols), and blocking such traffic for all other IP addresses.
- Enhancing detection/prevention capabilities by expanding coverage of intrusion-protection systems, updating signatures, and blocking network activity that indicates malicious behavior.
- Actively monitoring for suspicious activity – for example, identifying unusual increases in requests for fallback to vulnerable protocols – and responding appropriately.

Additionally, entities should ensure all applicable PCI DSS requirements are also in place, including:

- Proactively keeping informed about new vulnerabilities; for example, subscribing to vulnerability notification services and vendor support sites to receive updates about new vulnerabilities as they emerge.
- Applying vendor recommendations for configuring their technologies securely.

What are some migration options?

Examples of additional cryptographic measures that may be implemented and used as a security control to replace SSL/early TLS may include:

- Upgrading to a current, secure version of TLS that is implemented securely and configured to not accept fallback to SSL or early TLS.
- Encrypting data with strong cryptography before sending over SSL/early TLS (for example, using field-level or application-level encryption to encrypt the data prior to transmission)
- Setting up a strongly-encrypted session first (e.g. IPsec tunnel), then sending data over SSL within secure tunnel

Additionally, the use of two-factor authentication may be combined with the above controls to provide authentication assurance.

The choice of an alternative cryptographic control will depend on the technical and business needs for a particular environment.

What about small merchant environments?

All entity types are impacted by issues with SSL/early TLS, including small merchants. It is critical that small merchants take the necessary steps to remove SSL/early TLS from their cardholder data environment to ensure their customer data is secure.

For the POI environment, it is recommended that small merchants contact their terminal provider and/or acquirer (merchant bank) to determine if their POS POI terminals are affected by the SSL vulnerabilities.

For other environments – e.g. virtual payment terminals, back-office servers, user computers etc., small merchants should validate if SSL/early TLS is used and where it is implemented, and then determine if an upgrade can occur immediately, or if a business justification exists for a delayed upgrade (not to exceed June 30, 2018).

Suggestions for things to consider in your environment include:

- Check the web browser version your systems are using – older versions will use SSL/early TLS and you may need to upgrade to a newer browser
- Check firewall configurations to see if SSL can be blocked
- Check that all application and system patches are up to date
- Check and monitor systems to identify suspicious activity that may indicate a security issue

Additionally, when planning your migration to a secure alternative, you must complete a Risk Mitigation and Migration Plan.

What should merchants do with POI terminals that support SSL/early TLS?

POIs can continue using SSL/early TLS when it can be shown that the POI is not susceptible to the currently known exploits. However, SSL is an outdated technology and may be subject to additional security vulnerabilities in the future; it is therefore strongly recommended that POI environments use TLS v1.1 or greater wherever possible. New implementations of POIs should strongly consider support for and use of TLS 1.2 or greater. If SSL/early TLS is not needed in the environment, use of and fallback to these versions should be disabled.

When reviewing implementations of POI terminals that use SSL/early TLS, assessors should review supporting documentation (for example, documentation provided by the POI vendor, system/network configuration details, etc.) to determine if the implementation is susceptible to known exploits.

If the POS POI environment is susceptible to known exploits, then planning for migration to a secure alternative should commence immediately.

Note: The allowance for POS POIs that are not currently susceptible to exploits is based on current, known risks. If new exploits are introduced for which POI environments are susceptible, the POI environments will need to be updated.

Why are POS POI environments less vulnerable?

PCI DSS provides an allowance for SSL and early TLS to continue to be used by point of sale (POS) point of interaction (POI) devices and their termination points. This is because the vulnerabilities known at the time of publication are generally more difficult to exploit in these environments.

For example: Some of the current SSL vulnerabilities are exploited by an attacker intercepting the client/server communication and manipulating messages to the client. The attacker's goal is to deceive the client into sending additional data that the attacker can use to compromise the session. POS POI devices with the following characteristics are generally more resistant to this type of vulnerability:

- The device does not support multiple client-side connections (which facilitates the POODLE exploit).
- The payment protocol adheres to ISO 20022 (Universal Financial Industry Message Scheme)/ISO 8583-1:2003 (Financial Transaction Card Originated Messages – Interchange Message Specifications), or equivalent standard that limits the amount of data that can be exposed through "replay attacks".
- The device does not use web browser software, JavaScript, or security-related session cookies.

Note: These characteristics are intended as an example only; each implementation will need to be independently evaluated to determine the extent of susceptibility to vulnerabilities.

It is also important to remember that exploits continue to evolve and organizations must be prepared to respond to new threats. All organizations using SSL and/or early TLS should plan to upgrade to a strong cryptographic protocol as soon as possible.

Any interim use of SSL/early TLS in POS POI environments must have up-to-date patches, and ensure only the necessary extensions are enabled.

What does this mean for payment processors supporting POI environments?

Entities of all types are impacted by the SSL/early TLS issue, including payment processors, payment gateways, and other entities providing transaction processing services. These entities will need to review their use of SSL/early TLS and plan migrations in the same way as other entities.

Payment processing entities with POI termination points will need to verify the POI communications are not vulnerable (as described in the section "Why are POS POI environments less vulnerable", above) if they are to continue using SSL/early TLS.

If a payment processing entity supports multiple payment channels – for example, POI and e-commerce transactions – on the same termination point, the entity will need to ensure that all vulnerable channels are migrated to a secure alternative by June 30th, 2018. If the POI environment is deemed as being not susceptible to vulnerabilities, the entity may wish to consider the following options:

- Migrate POI channels to a secure alternative so both POI and e-commerce transactions can continue to use the same termination point.
- If POI channels are not being migrated, separate termination points/interfaces may be used to separate POI traffic that uses SSL/early TLS from e-commerce traffic that has been migrated to a secure alternative.

What about e-commerce environments?

Due to the nature of web-based environments, e-commerce implementations have the highest susceptibility and are therefore at immediate risk from the known vulnerabilities in SSL/early TLS.

Because of this, new e-commerce websites must not use or support SSL/early TLS.

E-commerce environments that have a current need to support customers using SSL/early TLS must begin migrating as soon as possible, with all migrations to be completed by 30th June, 2018. Where migration cannot occur immediately, the justification must be documented as part of the Risk Mitigation and Migration Plan.

Until the migration is complete, it is recommended that the number of servers supporting SSL/early TLS be minimized to as few as possible. Reducing the number of vulnerable systems reduces potential exposure to exploits, and may also help streamline risk mitigation controls, such as enhanced monitoring of suspicious traffic.

We also encourage e-commerce merchants to advise their customers to upgrade web browsers to support secure protocols.

Where to begin with the migration process?

Here are some suggested steps to help entities plan their migration to a secure alternative:

1. Identify all system components and data flows relying on and/or supporting the vulnerable protocols
2. For each system component or data flow, identify the business and/or technical need for using the vulnerable protocol
3. Immediately remove or disable all instances of vulnerable protocols that do not have a supporting business or technical need
4. Identify technologies to replace the vulnerable protocols and document secure configurations to be implemented
5. Document a migration project plan outlining steps and timeframes for updates
6. Implement risk reduction controls to help reduce susceptibility to known exploits until the vulnerable protocols are removed from the environment
7. Perform migrations and follow change control procedures to ensure system updates are tested and authorized
8. Update system configuration standards as migrations to new protocols are completed

Can SSL/early TLS remain in an environment if not used as a security control?

Yes, these protocols may remain in use on a system as long as SSL/early TLS is not being used as a security control.

Additionally, all SSL/TLS vulnerabilities that score CVSS 4 or higher on an ASV scan, or are ranked as "high" on an entity's internal vulnerability scan, must be addressed within the required timeframe (e.g. quarterly for ASV scans) in order to meet PCI DSS Requirement 11.2. Follow defined vulnerability management processes to document how SSL/TLS vulnerabilities are addressed – for example, where it is used only for POI communications that are not susceptible to the exploits, or where it is present but is not being used as a security control (e.g. is not being used to protect confidentiality of the communication).

Do the migration dates apply if there are no cardholder data compromises resulting from use of SSL/early TLS?

Yes, the date for migrating away from SSL/early TLS is not affected by the number of payment card data compromises that may or may not occur in the future. The PCI DSS requirements are intended to help prevent compromises of cardholder data through a defense-in-depth approach. Waiting for potential data breaches to be publicized before taking steps to secure your own data is not an effective approach to security, and is not supported in the PCI DSS.

How does the presence of SSL impact ASV scan results?

SSL v3.0 and early TLS contain a number of vulnerabilities, some of which currently result in a score of 4.3 on the CVSS (Common Vulnerability Scoring System). The CVSS is defined by NVD (National Vulnerability Database) and is the scoring system ASVs are required to use. Any Medium or High risk vulnerabilities (i.e. vulnerabilities with a CVSS of 4.0 or higher) must be corrected and the affected systems re-scanned after the corrections to show the issue has been addressed.

However, as there is no known way to remediate some of these vulnerabilities, the recommended mitigation is to migrate to a secure alternative as soon as possible. Entities that are unable to immediately migrate to a secure alternative should work with their ASV to document their particular scenario as follows:

- *Prior to June 30, 2018:* Entities that have not completed their migration should provide the ASV with documented confirmation that they have implemented a Risk Mitigation and Migration Plan and are working to complete their migration by the required date. Receipt of this confirmation should be documented by the ASV as an exception under "Exceptions, False Positives, or Compensating Controls" in the ASV Scan Report Executive Summary, and the ASV may issue a result of "Pass" for that scan component or host, if the host meets all applicable scan requirements.
- *After June 30, 2018:* Entities that have not completely migrated away from SSL/early TLS will need to follow the Addressing Vulnerabilities with Compensating Controls process to verify the affected system is not susceptible to the particular vulnerabilities. For example, where SSL/early TLS is present but is not being used as a security control (e.g. is not being used to protect confidentiality of the communication).

Entities with POS POI terminals and/or termination points that are verified as not being susceptible to the specific vulnerabilities may be eligible for a reduction in the NVD score for those systems. In this scenario, the ASV must provide (in addition to all the other required reporting elements), the following information in accordance with the ASV Program Guide:

- The NVD rating of the vulnerability
- The ASV's rating of the vulnerability
- Why the ASV disagrees with the NVD rating

For example, the ASV could determine that a specific vulnerability has a higher difficulty to exploit in a particular POS POI environment than that defined by the general NVD scoring system. The ASV may then re-rank this element of the scoring system for the specific vulnerability, for the systems in question.

When making any adjustments of this type, the ASV must consider the client's unique environment, systems and controls, and not make such adjustments based on general trends or assumptions. The scan customer should work with their ASV to provide an understanding of their environment; otherwise the ASV will be unable to determine whether changing a CVSS score is appropriate.

ASVs must exercise due diligence and due care when employing such concessions, and ensure there is sufficient evidence to support a change in the CVSS score. All such changes must follow the process defined in the ASV Program Guide.

All ASV Scan Reports must be completed in accordance with processes the ASV Program Guide.

Does this mean entities with a Risk Mitigation and Migration Plan don't have to patch vulnerabilities in SSL/early TLS?

No, the target migration dates are not an excuse to delay patching vulnerabilities. New threats and risks must continue to be managed in accordance with applicable PCI DSS Requirements, such as 6.1, 6.2, and 11.2, and entities must address vulnerabilities where a security update, fix, or patch is available.

What is the impact for services that support secure protocols (e.g. TLS v1.2) as well as insecure protocols (e.g. SSL/early TLS)?

Many service providers (for example, shared hosting providers) provide platforms and services for a broad base of customers, which may include entities that need to meet PCI DSS requirements as well as entities that do not. Service providers that support a customer's CDE can either demonstrate they are meeting the applicable requirements on behalf of the customer, or are providing service options that meet PCI DSS requirements for their customers to use. The service provider should clearly communicate to their customers which security protocols are offered, how to configure the different options, and the impact of using configurations considered to be insecure.

For example, a web hosting provider may offer a hosted web platform for merchants that supports TLS v1.2 and also supports weaker protocols. To support their customers' PCI DSS compliance, the hosting provider needs to provide clear instructions for the customer to configure their use of the service to use only TLS v1.2 with no fallback to SSL/early TLS. From the customer side, a merchant using this platform as part of their PCI DSS implementation will need to ensure the configuration options they are using include use of TLS v1.2 with no fallback to SSL/early TLS.

The presence of weaker protocols in a mixed-hosting environment may trigger a failure on the ASV scan. When this occurs, the service provider and ASV should follow the "Exceptions, False Positives, or Compensating Controls" process to document how the risk has been addressed – for example, by confirming SSL/early TLS is not being used as a security control by the service provider, and that secure configuration options that don't permit fallback to the weaker protocols are provided for customer use. The ASV may then issue a result of "Pass" for that scan component or host, if the host meets all applicable scan requirements.