INFORMATION SUPPLEMENT

Use of SSL/Early TLS for POS POI Terminal Connections

Date: June 2018
Author: PCI Security Standards Council

Table of Contents

Introduction

This Information Supplement provides guidance for merchants and service providers using SSL/early TLS for card-present POS POI terminal connections after June 30, 2018.

Additional guidance for other uses of SSL/early TLS and its impact on ASV scans is provided in the PCI SSC Information Supplement: ***Use of SSL/Early TLS and Impact on ASV Scans***.

Executive Summary

SSL/early TLS was removed as an example of strong cryptography in PCI DSS v3.1 (April 2015) and may not be used as a security control to meet any PCI DSS requirement after June 30, 2018. Methods to ensure that SSL/early TLS is not used as a security control include upgrading to a secure alternative or implementing compensating controls to mitigate the risk associated with the vulnerable protocols. An exception is provided for POS POI terminals that are verified as not being susceptible to known exploits and the termination points to which they connect, as defined in PCI DSS Appendix A2.

What is the risk?

SSL/TLS encrypts a channel between two endpoints (for example, between a point-of-sale (POS) point-of-interaction (POI) terminal and an acquirer or payment processor) to provide privacy and reliability of data transmitted over the communications channel. Since the release of SSL v3.0, several vulnerabilities have been identified—including POODLE (Padding Oracle On Downgraded Legacy Encryption), which is a man-in-the-middle attack that makes it 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.

What is meant by “Early TLS”?

The term “early TLS” was first introduced in PCI DSS v3.1 to address early implementations of the TLS protocol that contain protocol-level vulnerabilities. This approach was intended to help organizations identify and prioritize migration efforts for TLS implementations known to be inherently vulnerable. As threats continue to evolve and new versions of the protocol are released to address those threats, TLS implementations need to be kept up to date to prevent them becoming vulnerable to known exploits. To support this objective, the term “early TLS” does not refer to a specific version(s) of the protocol, but rather it encompasses any version or implementation of TLS that is vulnerable to a known exploit.

Where TLS is used as a security control for PCI DSS, the implementation will need to use and support modern cryptographic algorithms, secure configuration settings, and other features as needed in order to

meet the intent of strong cryptography. This means that every TLS implementation, irrespective of the protocol version, will need to be evaluated to determine whether it is appropriate to use as a security control for PCI DSS. Factors to consider when evaluating a TLS implementation include how it is configured, the services and options that are enabled, the cryptographic algorithms used and supported, and the cryptographic key strength. Entities using TLS should review their implementations against industry references (such as the current version of NIST SP 800-52) for guidance on configuration options that meet the intent of strong cryptography.

Note: *New vulnerabilities and exploits are constantly being discovered, and entities need to remain up to date with vulnerability trends to determine whether their implementation is or becomes susceptible to any known exploits. If new exploits are introduced that cannot be addressed with patches or compensating controls, entities will need to be able to update their systems to a secure alternative. Entities should therefore have a detailed understanding of their cryptographic implementations and have plans in place to take appropriate action in the event that protocols and/or algorithms in use require updating.*

What this means for PCI DSS

SSL and early TLS do not meet the intent of strong cryptography or secure protocols; therefore, they may not be used as security controls for PCI DSS. An exception is provided for both POS POI terminals that are verified as not being susceptible to known exploits and the termination points to which they connect, as defined in PCI DSS Appendix A2. Examples of PCI DSS requirements that may be affected by the use of SSL/early TLS include:

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.

Methods to ensure SSL/early TLS is not used as a security control include upgrading to a secure alternative or implementing compensating controls to provide the applicable security and mitigate the risk associated with the vulnerable protocol.

To support entities with POS POI terminal connections working to migrate away from SSL/early TLS, the following provisions are included:

- New POS POI terminal 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 POS POI terminal service providers must provide a secure TLS service offering.
- Service providers supporting existing POS POI terminal implementations that use SSL/early TLS must have a formal Risk Mitigation and Migration Plan in place.

- POS POI terminals in card-present environments that can be verified as not being susceptible to any known exploits for SSL and early TLS, and the SSL/TLS termination points to which they connect, may continue using SSL/early TLS as a security control.

If SSL/early TLS is used for POS POI terminal connections, the requirements in PCI DSS Appendix A2, "Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections," apply.

Note: *The allowance for POS POI terminals and their termination points does not extend to other systems or networks in the entity's environment. For example, merchants using SSL/early TLS on their POS POI terminals may not use these protocols as security controls for PCI DSS on any other system—such as virtual payment terminals, back-office servers, and user computers. Similarly, service providers of POS POI termination points should limit the presence of SSL/early TLS to only those termination points supporting POS POI connections. Service providers may not use SSL/early TLS as a security control for PCI DSS except as allowed in PCI DSS Appendix A2.*

Other than as allowed for POS POI terminal connections, can SSL/early TLS remain in an environment if not used as a security control?

While the recommended approach is to disable SSL and early TLS entirely and migrate to a more modern encryption protocol, these protocols may remain in use on a system as long as they are not used as security controls to meet a PCI DSS requirement.

All SSL/TLS vulnerabilities with a CVSS (Common Vulnerability Scoring System) score of 4.0 or higher on an ASV scan or that are ranked as "high" on an 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. Additionally, new threats and risks must continue to be managed in accordance with applicable PCI DSS Requirements for patching and vulnerability management (Requirements 6.1, 6.2).

Examples of additional cryptographic measures that may be implemented to replace SSL/early TLS as a security control 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 the secure tunnel

The use of multi-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.

Why are POS POI terminals 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 many of these types of systems.

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 facilitate 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 examples 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/early TLS for POS POI terminal connections should plan to upgrade to a strong cryptographic protocol as soon as possible.

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

Understanding "new" and "existing" implementations

Implementations are considered "new" 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.

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.

What this means for merchants with POS POI terminals that support SSL/early TLS

POS POI terminals can continue using SSL/early TLS when it can be shown that the terminal is not susceptible to 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 terminals use a secure version of TLS wherever possible. If SSL/early TLS is not needed in the environment, use of and fallback to these versions should be disabled. New implementations of POS POI terminals should not support SSL or early TLS.

If the POS POI terminals become susceptible to known exploits, 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 to which POI terminals are susceptible the POI terminals will need to be updated immediately.*

Confirming that POS POI terminals are not susceptible to known exploits for SSL/early TLS

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

Many POS POI vendors provide lists of which of their devices are susceptible to known SSL/early TLS exploits. Merchants are encouraged to consult with their POI terminal provider or vendor for information on their particular devices. The merchant may also wish to consult with knowledgeable security professionals for assistance obtaining verification.

The verification that POS POI terminals are not susceptible will need to occur every time a new SSL/TLS vulnerability is discovered. Organizations will need to remain up to date with vulnerability trends to determine whether they are susceptible to any known exploits. Additionally, new threats and risks must also continue to be managed in accordance with applicable PCI DSS Requirements for patching and vulnerability management.

It should also be noted that if (and when) a new vulnerability is discovered that exploits POS POI terminal implementations, merchants and their service providers will need to migrate immediately to a secure option.

What about small merchant environments?

All entity types, including small merchants, are impacted by issues with SSL/early TLS. 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 POS POI terminal environment, it is recommended that small merchants contact their terminal provider and/or acquirer (merchant bank) to determine whether their POS POI terminals are affected by the SSL/early TLS vulnerabilities.

For other environments—e.g., virtual payment terminals, back-office servers, user computers etc., small merchants should validate that SSL/early TLS is not used.

Reporting the use of SSL/early TLS as a security control in POS POI terminals

Entities (such as merchants) with existing POS POI terminal implementations that use SSL/early TLS as a security control will need to document this usage in their Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ), as applicable.[1]

The use of SSL/early TLS in POS POI terminals should be reported in in PCI DSS Appendix A2 and in any PCI DSS requirement(s) for which SSL/early TLS is relied on as a security control, as described below.

- Confirm all POS POI terminals using or supporting SSL/early TLS are not susceptible to any known exploits for those protocols. Once confirmed, document Requirement A2.1 as being “In Place” in the ROC or select “Yes” in the SAQ. When completing a ROC, include details of how Requirement A2.1 was verified as being in place in the “Reporting Details: Assessor’s Response” column.

[1] As defined by payment brand compliance programs.

- Once Requirement A2.1 is confirmed for all POS POI terminals, any PCI DSS requirement for which SSL/early TLS is used a security control may be considered "In Place" (or "Yes" in a SAQ) for those terminals. When completing a ROC, document in the applicable requirement that all POS POIs using SSL/early TLS have been verified as not being susceptible to known exploits and refer to Requirement A2.1 for details.

What this means for service providers with existing termination points for POS POI terminals

Service providers with existing termination points to POS POI terminals—for example, an acquirer or acquirer processor, payment processor, payment gateway, or other entity providing transaction processing services—may continue using SSL/early TLS for those connections, as long as the service provider has controls in place to mitigate the risk of supporting those connections for the service provider environment.

All service providers with existing connection points to POS POI terminals are required to have a formal Risk Mitigation and Migration Plan in place, including a future date for migration to a secure alternative. Service providers should communicate the risks associated with the use of SSL/Early TLS and the future date for completion of the migration to their POS POI terminal customers.

Additionally, SSL/TLS vulnerabilities that score CVSS 4.0 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. New threats and risks must continue to be managed in accordance with applicable PCI DSS Requirements for patching and vulnerability management (Requirements 6.1, 6.2).

Confirming that SSL/early TLS is accepted only for POI terminal connections

If a service provider supports multiple payment channels—for example, POI and e-commerce transactions—the service provider will need to ensure that SSL/early TLS is disabled on all e-commerce and any other vulnerable channels. The service provider may also wish to consider the following options:

- Migrate POI channels to a secure alternative so both POI and e-commerce transactions can use the same secure termination points.
- If POI channels have not been migrated, use dedicated termination points/interfaces to separate POS POI terminal traffic that uses SSL/early TLS from e-commerce traffic that has been migrated to a secure alternative.

Preparing a Risk Mitigation and Migration Plan

The Risk Mitigation and Migration Plan is a document prepared by service providers supporting existing SSL/early TLS connection points to POS POI terminals. The Risk Mitigation and Migration Plan details the service provider's plans for migrating to a secure protocol and also describes controls 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:
  - Service providers 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:
  - Service providers need to be proactive and stay informed about new vulnerabilities. As new vulnerabilities are published, the service provider needs to evaluate the risk posed to its environment and determine whether 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 a service provider does not currently use or need to support vulnerable protocols, there is no reason why it should introduce such protocols to its environment. Change-control processes include evaluating the impact of the change to confirm it does not introduce a new security weakness into the environment.
- Overview of migration project plan to replace SSL/early TLS at a future date:
  - 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.

- In determining a future date for completing migration from SSL/early TLS, the service provider will need to consider a number of factors, including the size and complexity of the environment, the security needs of the organization, communication channels, hardware replacement cycles, the current threat environment, and the likelihood of new critical vulnerabilities being discovered that affect these vulnerable protocols.

Communication to POS POI customers

Implementation of a customer communication strategy is recommended as part of the Risk Mitigation and Migration Plan, to help educate POS POI customers about the dangers of using outdated protocols and the associated risk to the their data and systems. Service providers should communicate to all POS POI customers using SSL/early TLS about the need to migrate to a secure protocol, as well as the future date associated with the service provider's migration plan.

Provision of a Secure Service Offering

Service providers supporting SSL/early TLS connections for POS POI terminals are also required to provide a secure protocol option for their POS POI terminal customers. The service provider should provide clear information to its customers about the security protocols offered, how to activate and configure the different options, and the impact of using configurations considered to be insecure.

Service providers may provide a termination point that supports POS POIs using a secure version of TLS as well as POS POIs using SSL/early TLS. To support customers that are using a secure version of the protocol, the service provider needs to provide clear instructions for customers about how to configure their use of the service to support only the secure version with no fallback to SSL/early TLS.

Reporting the use of SSL/early TLS as a security control for POS POI termination points

Service providers supporting existing SSL/early TLS connections to POS POI terminals will need to document this usage in their Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ), as applicable.[2]

The use of SSL/early TLS to support POS POI terminal connections should be reported in PCI DSS Appendix A2 and in any PCI DSS requirement(s) for which SSL/early TLS is relied on as a security control, as described below

- Confirm that the SSL/early TLS connection points are provided only for POS POI terminal connections.
- Confirm a Risk Mitigation and Migration Plan is in place in accordance with Requirement A2.2. Once confirmed, document Requirement A2.2 as being "In Place" in the ROC or select "Yes" in the SAQ. When

[2] As defined by payment brand compliance programs.

completing a ROC, include details of how Requirement A2.2 was verified as being in place in the "Reporting Details: Assessor's Response" column.

- Confirm a secure service offering is provided for POS POI terminal customers, in accordance with Requirement A2.3. Once confirmed, document Requirement A2.3 as being "In Place" in the ROC or select "Yes" in the SAQ. When completing a ROC, include details of how Requirement A2.3 was verified as being in place in the "Reporting Details: Assessor's Response" column.
- Once Requirements A2.2 and A2.3 are confirmed, any PCI DSS requirement for which SSL/early TLS is used as a security control for existing POS POI termination connections may be considered "In Place" for those connections. When completing a ROC, document in the applicable requirement that the SSL/early TLS connection points are provided only for POS POI terminal connections and refer to Requirements A2.2 and A2.3 for details.

Additional Risk Mitigation and Migration Guidance

What are risk mitigation controls?

For environments currently using vulnerable protocols, the implementation and continued use of risk mitigation controls help 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 associated with POS POI terminals still using 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 or increases in the volume of HTTP requests from the same source—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

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 still 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. Confirm that all instances of vulnerable protocols that do not have a supporting business or technical need have been removed or disabled.
4. Identify technologies to replace the vulnerable protocols and document secure configurations to be implemented.
5. Establish a date for the completion of the migration.
6. Document a migration project plan outlining steps and timeframes for updates.
7. Review the implementation of controls that mitigate the risk of supporting those connections for the environment until migration can be completed.
8. Communicate to all customers using SSL/early TLS about the risks associated with its use and the need to migrate to a secure protocol. Communicate the future date for the completion of the migration from SSL/early TLS.
9. Perform migrations and follow change-control procedures to ensure system updates are tested and authorized.
10. Update system configuration standards as migrations to new protocols are completed.

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

No, setting a target migration date is 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.