INFORMATION SUPPLEMENT

Use of SSL/Early TLS and Impact on ASV Scans

Date: June 2018
Author: PCI Security Standards Council

Table of Contents

Introduction

This Information Supplement provides guidance on the use of SSL/early TLS and its impact on PCI DSS and ASV Scan results after June 30, 2018.

Additional guidance for merchants and service providers using SSL/early TLS for card-present POS POI terminal connections after June 30, 2018 is provided in the PCI SSC Information Supplement: ***Use of SSL/Early TLS for POS POI Terminal Connections***.

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 both POS POI terminals that are verified as not susceptible to known exploits and the termination points to which they connect, as defined in PCI DSS Appendix A2.

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. Examples of applicable PCI DSS requirements 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.

SSL/early TLS may not be used as a security control to meet these or any other PCI DSS requirement. 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. 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.

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.

How does the presence of SSL/early TLS impact ASV scan results?

SSL and early TLS contain a number of vulnerabilities that score 4.0 or higher 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, in accordance with the current version of the ASV Program Guide. As defined in PCI DSS Requirement 11.2.2, 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.

The ASV Program Guide requires that a component be marked as an automatic failure by the ASV if:

- The component supports SSL or early versions of TLS, or
- The component supports strong cryptography in conjunction with SSL or early versions of TLS (due to the risk of “forced downgrade” attacks).

As described in the ASV Program Guide, ASV scans must identify all vulnerabilities with a CVSS of 4.0 or higher and mark such instances as scan failures. Scan customers using SSL/early TLS for purposes other than as a security control for PCI DSS or that have implemented additional controls to mitigate the risk of the vulnerabilities associated with using SSL/early TLS may follow the “Managing False Positives and Other Disputes” or “Addressing Vulnerabilities with Compensating Controls” process, as applicable. Both of these processes are defined in the ASV Program Guide. The ASV can then assess the relevance and applicability of the information provided by the scan customer and potentially change the finding for the affected component to a “Pass.”

This process requires the scan customer to provide the ASV with sufficient information, including supporting evidence as needed, about why the presence of SSL/early TLS should not result in a failure for the affected component—for example, details of the additional controls implemented or environment-specific factors that

reduce or eliminate the risk posed by the identified vulnerabilities. Details of the compensating controls or other mitigating factors should be documented in "Exceptions, False Positives, or Compensating Controls" section of the ASV Scan Report.

ASVs may also re-rank a vulnerability's risk assignment if they are able to confirm that the risk level is lower in a particular environment. When making this type of adjustment to the scan report, the ASV should consider the scan customer's unique environment, systems, and controls, and not make adjustments based on general trends or assumptions.

In all cases, scan customers and ASVs should work together to determine the level of risk that a particular vulnerability may present in a specific environment or configuration. All ASV Scan Reports must be completed in accordance with processes described in the ASV Program Guide. Refer to the following sections in the ASV Program Guide for details of these processes:

- Section 7.7 "Managing False Positives and Other Disputes"
- Section 7.8 "Addressing Vulnerabilities with Compensating Controls".

Additional considerations for specific scenarios are outlined below.

Reporting ASV Scans

Where SSL/early TLS is used as a security control

Entities that continue to use SSL/early TLS as a security control for an in-scope system component and have implemented compensating controls to mitigate the risk of using SSL/early TLS should provide the ASV with sufficient information to confirm that the risks associated with using SSL/early TLS have been mitigated—for example, through the use of additional cryptographic mechanisms or additional security controls. Once the entity has provided the ASV with sufficient information and supporting evidence, as needed, and if all applicable scan requirements are met, the ASV may then issue a result of "Pass" for that scan component.

Entities that are using SSL/early TLS as a security control for PCI DSS and have ***not*** implemented compensating controls to mitigate the risk of using SSL/early TLS will likely not be able to achieve a passing scan for the affected components.

Where SSL/early TLS is present but not used as a security control

Where SSL/early TLS exists in an environment but is not being used as a security control, the entity should provide the ASV with sufficient information to verify that the presence of SSL/early TLS does not affect the security of any in-scope system and is not being used to meet any PCI DSS requirement (e.g., is not being used to protect confidentiality of the communication). Once the entity has provided the ASV with sufficient information and supporting evidence, as needed, and if all applicable scan requirements are met, the ASV may then issue a result of "Pass" for that scan component.

For POS POI terminals using SSL/early TLS as a security control

Entities with POS POI terminals using SSL/early TLS that have been confirmed as not being susceptible to known exploits should provide the ASV with sufficient information to verify:

- SSL/early TLS is used only by POS POI terminals in accordance with PCI DSS Appendix A2;
- The entity is not otherwise using SSL/early TLS as a security control; and
- Each POS POI terminal using SSL/early TLS has been verified as not being susceptible to any known SSL/early TLS exploits, including those with a score of CVSS 4.0 or higher that are identified in the ASV scan.

Once the entity has provided the ASV with sufficient information and supporting evidence, as needed, and if all applicable scan requirements are met, the ASV may then issue a result of "Pass" for that scan component.

Entities with POS POI terminals that are verified as not being susceptible to the specific vulnerabilities may also 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 in the general NVD/CVSS. The ASV may then re-rank this element of the scoring system for the specific vulnerability, for each system 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 its ASV to provide an understanding of its 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.

For service providers supporting POS POI terminals using SSL/early TLS

Service providers of connection points for POS POI terminals that use SSL/early TLS should provide the ASV with sufficient information to verify:

- The use of SSL/early TLS is only to support existing connections from POS POI terminals in accordance with PCI DSS Appendix A2, and the provider is not otherwise using SSL/early TLS as a security control;
- The service provider has a formal Risk Mitigation and Migration Plan in place to replace SSL/early TLS at a future date;
- Risk-reduction controls are in place to mitigate the risk of supporting those connections for the service provider environment; and
- A secure service offering that does not permit fallback to the weaker protocols is provided to POS POI terminal customers.

Once the entity has provided the ASV with sufficient information and supporting evidence, as needed, and if all applicable scan requirements are met, the ASV may then issue a result of "Pass" for that scan component.

Considerations for services that support secure protocols as well as SSL/early TLS

Many service providers (for example, shared hosting providers) provide platforms and services for a broad base of customers. Not all of these customers will need to use PCI DSS compliant options provided by the service provider. Service providers that support a customer's CDE can demonstrate either that they are meeting the applicable PCI DSS 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 its customers which security protocols are offered, how to configure the different options, and the impact of using configurations considered to be insecure.

The service provider should also inform customers using SSL/early TLS about the risks associated with its use and the need to migrate to a secure protocol. Communication should include a future date for migration away from SSL/early TLS—that is, the date from which the service provider will stop supporting these insecure protocols.

For example, a hosting provider may offer a hosted web platform for merchants that supports a secure version of TLS and also supports weaker protocols. To support its customers' PCI DSS compliance, the hosting provider needs to provide clear instructions for the customer to configure its use of the service to use only the secure version of TLS with no fallback to SSL/early TLS. From the customer side, a merchant using this platform as part of its PCI DSS implementation will need to ensure the configuration options it is using include use of secure TLS 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 "Managing False Positives and Other Disputes" or "Addressing Vulnerabilities with Compensating Controls" process,[1] as applicable, 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 do not 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.

[1] Refer to ASV Program Guide.