

Bulletin on Migrating from SSL and Early TLS

A Resource Guide from the PCI Security Standards Council

The Payment Card Industry Security Standards Council (PCI SSC) is **extending the migration completion date to 30 June 2018** for transitioning from Secure Sockets Layer (SSL) and Transport Layer Security (TLS) v1.0 to a secure version of TLS (currently v1.1 or higher).

These dates provided by PCI SSC as of **December 2015 supersede** the original dates issued in both PCI Data Security Standard v3.1 (PCI DSS 3.1) and in the [Migrating from SSL and early TLS](#) Information Supplement in April 2015.

Read on for answers to questions about new timelines, requirements and reasons for the adjustments. Thank you to all who have provided feedback on the issue, including members of the National Institute of Standards & Technology (NIST), members of the Financial Services Information Sharing Analysis Center (FS-ISAC), Retail Solution Providers Association, Hotel Technology Next Generation, National Restaurant Association and Retail Industry Leaders Association.

In addition to the answers below, more information can be found by viewing the [SSL/TLS Migration webcast](#).

PCI DSS 3.1:
SSL/Early TLS
No Longer Secure



HOW BIG IS THE RISK?

The vulnerabilities within SSL and early TLS are serious. A slew of high-profile breaches caused by POODLE, Heartbleed and Freak are due to weaknesses within the protocols.



18 months after the Heartbleed vulnerability was announced, it was reported that there still was

200,000+ **VULNERABLE DEVICES**
on the internet.



In November 2015,
67% of sites surveyed had
INADEQUATE SECURITY

Source: [TrustworthInternet.org](#)

ACTION ITEMS FOR YOUR ORGANIZATION

In April 2015, PCI SSC issued initial guidance and removed SSL as an example of strong cryptography from the PCI Data Security Standard (PCI DSS), stating that it can no longer be used as a security control after 30 June 2016. **After seeking extensive marketplace feedback, the PCI Security Standards Council revised and updated sunset dates.**

In total, the revisions state:

- All processing and third party entities – including Acquirers, Processors, Gateways and Service Providers must provide a TLS 1.1 or greater **service offering** by June 2016
- Consistent with the existing language in the DSS v3.1, all **new implementations** must be enabled with TLS 1.1 or greater
- All processing and third party entities must cutover to a secure version of TLS (as defined by NIST) effective **June 2018**
- The use of SSL/TLS 1.0 **within a POI terminal** that can be verified as **not being susceptible** to all known exploits for SSL and early TLS, with no demonstrative risk can be used **beyond June 2018** consistent with the existing language in the DSS v3.1 for such an exception

FREQUENTLY ASKED QUESTIONS ON SSL AND EARLY TLS

Q Why change the original date for SSL included in PCI DSS v3.1?

A: For more than 20 years Secure Sockets Layer (SSL) has been one of the most widely-used encryption protocols. It remains in widespread use today despite existence of a number of security vulnerabilities and being deprecated **by NIST in 2014**.

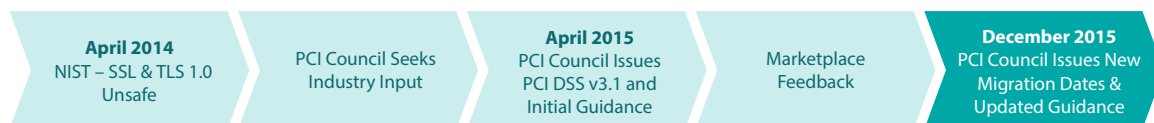
According to NIST, there are no fixes or patches that can adequately repair SSL or early TLS. Therefore, it is critically important that organizations upgrade to a secure alternative as soon as possible, and disable any fallback to both SSL and early TLS.

In April 2015, after extensive marketplace feedback, PCI SSC removed SSL as an example of strong cryptography from the PCI Data Security Standard (PCI DSS) v3.1, stating that it can no longer be used as a security control after 30 June 2016. During the implementation period of PCI DSS v3.1, PCI SSC continued to seek feedback from the market, and has now **revised and updated sunset dates**.

The **new date of June 2018** offers additional time to migrate to more secure protocols, but **waiting is not recommended**. The existence of the POODLE and Heartbleed exploits, among others, prove that anyone using SSL and early TLS risks being breached.

In total, the revisions state:

1. All processing and third party entities – including Acquirers, Processors, Gateways and Service Providers must provide a TLS 1.1 or greater **service offering** by June 2016.
2. Consistent with the existing language in PCI DSS v3.1, all **new implementations** must be enabled with TLS 1.1 or greater. TLS 1.2 is recommended. (New implementations are **when there is no existing dependency** on the use of the vulnerable protocols – see PCI SSC Information Supplement: Migrating from SSL and Early TLS.)
3. All entities must cutover to use only a secure version of TLS (as defined by NIST) effective **30 June 2018** (with the following exception).
4. The use of SSL/early TLS **within a Point of Interaction (POI) terminal and its termination point** that can be verified as **not being susceptible** to all known exploits for SSL and early TLS, with no demonstrative risk, can be used **beyond June 2018** consistent with the existing language in PCI DSS v3.1 for such an exception.



Q What is the PCI Standards Security Council doing next?

A: PCI DSS v3.1 will be updated in 2016. Information supplements and additional guidance will also be updated at this time.

UNDERSTANDING THE RISK

Q What is SSL/TLS?

A: Transport Layer Security (TLS) is a cryptographic protocol used to establish a secure communications channel between two systems. It is used to authenticate one or both systems, and protect the confidentiality and integrity of information that passes between systems.

Q What is the history of SSL/TLS?

A: TLS was originally developed as SSL- Secure Sockets Layer by Netscape in the early 1990s. Standardized by the Internet Engineering Taskforce (IETF), TLS has undergone several revisions to improve security to block known attacks and add support for new cryptographic algorithms, with major revisions to SSL 3.0 in 1996, TLS 1.0 in 1999, TLS 1.1 in 2006, and TLS 1.2 in 2008.

Q What are the SSL/TLS Vulnerabilities?

A: Because of its widespread use online, SSL and TLS have been targeted by security researchers and attackers. Many vulnerabilities in SSL and TLS have been uncovered over the past 20 years.

Q What are the different classes of vulnerabilities?

- A: Protocol Vulnerabilities: There are many! Cryptographic vulnerabilities in either the SSL/TLS protocol itself, or in how it uses cryptographic algorithms. e.g., POODLE, BEAST, CRIME.
- Implementation Vulnerabilities: Vulnerabilities in TLS software. E.g., Heartbleed's Buffer over-read vulnerability in OpenSSL.
- Configuration Vulnerabilities: e.g., weak cipher suites or key sizes. Logjam attacks using export-grade cryptography.

Q What are the impacts of vulnerabilities?

- A: Loss of confidentiality or integrity: Many of the attacks, particularly protocol vulnerabilities, allow for Man-in-the-Middle attacks allowing an attacker to decrypt sensitive information.
- Loss of cryptographic keys: In some of the most serious cases, vulnerabilities could allow an attack to steal long-lived cryptographic keys.

Q Who is most susceptible to SSL vulnerabilities?

- A: Online and e-commerce environments using SSL (and early versions of TLS) are most susceptible to the SSL exploits and attacks and should be upgraded immediately. With that being said, the PCI DSS migration date of 30 June 2018 applies to all environments (except for POI environments as stated above).

Q What you can and should do now?

- A: **Migrate to a minimum of TLS 1.1, preferably TLS 1.2.** While it is possible to implement countermeasures against some attacks on TLS, migrating to a later version of TLS - notably TLS 1.1 and TLS 1.2 - is the only reliable method to protect yourself from the current protocol vulnerabilities.

Patch TLS software against implementation vulnerabilities. Implementation vulnerabilities, such as Heartbleed in OpenSSL, can pose serious risks. Keep your TLS software up-to-date to ensure you are patched against these vulnerabilities, and have countermeasures for other attacks.

Configure TLS securely. In addition to providing support for later versions of TLS, ensure your TLS implementation is configured securely. Ensure you're supporting secure TLS cipher suites and key sizes, and disable support for other cipher suites that are not necessary for interoperability. For example, disable support for weak "Export-Grade" cryptography, which was the source of the recent Logjam vulnerability.

Q If my payment terminals (POIs) use SSL or TLS 1.0 for encryption, do I need to replace my payment terminals?

- A: **Not necessarily.** POIs are currently not as susceptible to the same known vulnerabilities as browser-based systems. Therefore, after 30 June 2018, POI devices (and the termination points to which they connect) that can be verified as not being susceptible to any of the known exploits for SSL and early versions of TLS may continue to use SSL / early TLS.
- If SSL/early TLS is used,** the POIs and their termination points must have up-to-date patches, and ensure only the necessary extensions are enabled.
- Additionally, **use of weak cipher suites** or unapproved algorithms – e.g., RC4, MD5, and others – is NOT allowed.

Q Who can verify my POIs meet the above characteristics?

- A: **Entities may contact the terminal vendors directly** for evidence or attestation that payment devices are not susceptible to known vulnerabilities. Entities may also consult with knowledgeable security professionals to obtain verification. The verification will need to occur any time a new SSL/TLS vulnerability is discovered, and organizations will need to remain up-to-date with vulnerability trends to determine whether or not they are susceptible to any known exploits. 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.

Q Do all POIs use SSL for encryption?

- A: **No.** Newer payment devices should already be using secure protocols such as TLS version 1.2. Check with the terminal manufacturer or terminal documentation to understand what level of encryption your particular POI uses. If a device does not need to support SSL/early TLS, disable both use of and fallback to these versions.

Q My ASV scan is flagging the presence of SSL and my scan is failing. What should I do?

A: **Prior to 30 June 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.

After 30 June 2018: Entities that have not completely migrated away from SSL/early TLS will need to follow the process outlined in the ASV Program Guide section entitled “Managing False Positives and Other Disputes” to confirm 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).

Q Does this mean that I don't have to address this vulnerability until 2018?

A: **No**, this is not an excuse to delay addressing vulnerabilities. You should be fixing those vulnerabilities that have patches.

Q What if a new attack is discovered on a current version of TLS?

A: It is always important to focus on security and keep track of new vulnerabilities. Technology and threats are constantly evolving. When new vulnerabilities are discovered they need to be addressed and may result in a need to upgrade to a newer, more secure version of the TLS protocol. Future-planning is vital to stay protected. Implement strong options now is the recommended action. PCI DSS already requires organizations to keep systems protected from vulnerabilities.

Q What about Approved Scanning Vendors and how this impacts ASV scans?

A: We're aware that some current SSL vulnerabilities trigger a CVSS, Common Vulnerability Scoring System, score of 4.3. Any medium to high vulnerabilities, CVSS of 4.0 or higher, must be corrected and rescanned to ensure the vulnerability has been addressed.

However, because there are no known ways to address some SSL/early TLS vulnerabilities, it makes it difficult to correct and rescan as with other vulnerabilities.

Prior to 30 June 2018, we recommend every entity work with their ASV and provide their migration plan as discussed previously. The ASV can document receipt of this plan under the “Exceptions, False Positives, or Compensating Controls” section of the ASV scan report.

After 30 June 2018, if the entity still has SSL or early TLS in its environment, the entity will need to document that its systems have been verified as not susceptible to the vulnerability and complete the Addressing Vulnerabilities with Compensating Controls process for their particular environment.

For POS POI environments, where it has been **verified that terminals are not susceptible to current SSL vulnerabilities**, the ASV has the discretion to change the CVSS score for a specific vulnerability as long as they follow the defined process in the ASV program guide and provide justification for the change. It's important for the ASV to consider the clients unique environment before making any changes.

Q What goes into creating a risk mitigation and migration plan?

A: **A risk mitigation and migration plan** details how an entity will address the migration to a secure protocol, including the controls in place to reduce risk associated with SSL and early TLS, until its migration is complete. The plan will need to be provided to an assessor during an entity's PCI DSS assessment. An assessor can then check the progress of the plan if a Report on Compliance (ROC) is completed prior to June 2018.

Q Can you give some examples of information that may need to be included in the risk mitigation and migration plan?

A: **A description of how vulnerable protocols are being 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 – for example does it include 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.

The **risk assessment results and risk reduction controls** currently in place:

- Entities should have evaluated and documented the risk to its environment and have implemented risk reduction controls to help mitigate the risk until the vulnerable protocols can be completely removed.

A 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 its environment and determine if additional risk reduction controls need to be implemented until the migration is complete.

A 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 it 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.

An **overview of migration project plan** including target migration completion date **no later than 30 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 30 June 2018.

Q Where do you begin with the migration process?

A: **Some key points to consider** are:

- Identify all system components and data flows relying on and/or supporting the vulnerable protocols
- For each system component or data flow, identify the business and/or technical need for using the vulnerable protocol
- Immediately remove or disable all instances of vulnerable protocols that do not have a supporting business or technical need
- Identify technologies to replace the vulnerable protocols and document secure configurations to be implemented
- Document a migration project plan outlining steps and timeframes for updates
- Implement risk reduction controls to help reduce susceptibility to known exploits until the vulnerable protocols are removed from the environment
- Perform migrations and follow change control procedures to ensure system updates are tested and authorized
- Update system configuration standards as migrations to new protocols are completed
- It is important to build a communications element into migration planning. Consider how much leg work it will take to get agreement on changing


The PCI Council has published very specific guidance on interim risk mitigation approaches, migration recommendations and alternative options for strong cryptographic protocols, including FAQs and tips for small merchant environments, all available on the website. The information supplement will be updated with the new dates. However, the guidance in it is still relevant and helpful; please review it for valuable content realizing that the dates will be updated.

Q I am a small merchant and/or franchisee and my employees are not security professionals. Where can I get additional support?

A: It is recommended that small merchants and franchisees **work with their acquiring bank** to determine whether their environment is at risk for SSL or early versions of TLS vulnerabilities.

IN-DEPTH BACKGROUND MATERIALS

**WEBINAR:
MIGRATING FROM SSL
AND EARLY TLS**



Please join the PCI Council, NIST and members of the assessor community for this 60-minute session that will provide guidance on making this important transition to protect your data and your customers.

[View now](#)




Payment Card Industry (PCI)
Data Security Standard

Summary of Changes from
PCI DSS Version 3.0 to 3.1

April 2015

[pdf Summary of Changes from PCI DSS Version 3.0 to 3.1](#)



INFORMATION SUPPLEMENT

Migrating from SSL and Early TLS

Version 1.0
Date: April 2015
Author: PCI Security Standards Council

[pdf Information Supplement: Migrating from SSL and Early TLS](#)

NIST Special Publication 800-52
Revision 1

Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

Tim Polk
Kerry McKay
Samosh Chokhani

<http://dx.doi.org/10.6028/NIST.SP.800-52-1>

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

[pdf National Institute of Standards and Technology: Guidelines for the Selection, Configuration, and Use of Transport Layer Security \(TLS\) Implementations](#)


Source: nist.gov

RELATED RESOURCES



[www What are secure websites and SSL/TLS certificates?](#)

Source: Indiana University



Interested in learning more about security?

**SANS Institute
InfoSec Reading Room**

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

SSL and TLS: A Beginners Guide

[pdf SSL and TLS: A Beginners Guide](#)

Source: SANS.org

Media: for expert comment, please contact:

press@pcisecuritystandards.org

For more information on PCI Standards and resources, visit: www.pcisecuritystandards.org