Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

PCI SSC FAQ on impending revisions to PCI DSS, PA-DSS to address SSL protocol vulnerability

25 March 2015

***Note: This document provides additional information to support the "PCI SSC bulletin on impending revisions to PCI DSS, PA-DSS", 13 February 2015.**

Why does SSL need to be removed as an example of "strong cryptography" from the PCI DSS and PA-DSS?
The National Institute of Standards and Technology (NIST) has identified the Secure Socket Layers (SSL) v3.0 protocol (a cryptographic protocol designed to provide secure communications over a computer network) as not being acceptable for the protection of data due to inherent weaknesses within the protocol. Because of these weaknesses, no version of the SSL protocol meets the PCI Security Standards Council (PCI SSC) definition of "strong cryptography," and revisions to the PCI Data Security Standard (PCI DSS) and the Payment Application Data Security Standard (PA-DSS) are necessary. The successor protocol to SSL is TLS (Transport Layer Security) and its most current version as of this publication is TLS 1.2. TLS 1.2 currently meets the PCI SSC definition of "strong cryptography".

How does it pose a risk to payment card data?
The SSL protocol vulnerability primarily affects web servers and browsers, so if exploited it can jeopardize the security of any payment card data being accepted or processed. Upgrading to a current, secure version of TLS, the successor protocol to SSL, is the only known way to remediate the SSL vulnerabilities which have been most recently exploited by browser attacks including POODLE and BEAST.

How does it impact the security of PIN Transaction Security (PTS) Point-of-Interaction (POI) terminals?
PTS POI terminals (devices such as a magnetic card readers or chip card readers that enable a consumer to use a payment card to make a purchase) can be impacted if the software on these terminals is communicating using the SSL protocol. As known vulnerabilities are difficult to exploit in this environment, the Council considers this a lower priority risk compared to web servers and browsers. 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.

Which requirements does it potentially impact?
The changes impact all requirements in the PCI DSS and PA-DSS that reference SSL as an example of "strong cryptography". Specifically:

- PCI DSS Requirements 2.2.3, 2.3 and 4.1
- PA-DSS Requirements 6.2, 8.2, 11.1 and 12.1-12.2

Which documents will be affected?
As these are revisions to the standards, all PCI DSS and PA-DSS v3.0 documentation will be affected, including: Self-Assessment Questionnaires (SAQ), Attestation of Compliance (AOC), Report on Compliance (ROC), Attestation of Validation (AOV) and Report on Validation (ROV).

When will the PCI DSS and PA-DSS 3.1 revisions be published?
The Council plans to publish the revision for PCI DSS in April, with the PA-DSS revision to follow shortly after.

When published, the revisions will be effective immediately but impacted requirements will have a sunset date to allow for organizations with affected systems to implement the changes. The Council will provide guidance on risk mitigation approaches to be applied during the migration process. For PA-DSS v3.1, the Council is also looking at how to address both future submissions and currently listed applications. The revised standards will be accompanied by a summary of changes document for each standard, as well as supporting guidance to help clarify the impact of these changes,

including interim risk mitigation approaches, migration recommendations and alternative options for strong cryptographic protocols.

How is the Council recommending organizations address this vulnerability?
Per the PCI SSC Bulletin on Impending Revisions to PCI DSS, PA-DSS, the Council urges organizations to work with your IT departments and/or partners to understand if and how your systems are using SSL and to determine available options for upgrading to at least TLS 1.1 or higher as soon as possible.

When publishing the revisions, the Council will also provide guidance and educational webinars on the use of interim risk mitigation approaches, migration recommendations and alternative options for strong cryptographic protocols.

***