Media Contacts

Lindsay Goodspeed
PCI Security Standards Council
+1-781-258-5843
press@pcisecuritystandards.org
Twitter @PCISSC

Payment Card Industry
Security Standards Council, LLC

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

PCI COUNCIL PUBLISHES REVISION TO PAYMENT APPLICATION DATA SECURITY STANDARD

— Organizations urged to upgrade their payment applications to protect against vulnerabilities in SSL protocol that can put payment data at risk —

WAKEFIELD, Mass., 1 June 2015 — Today, the PCI Security Standards Council (PCI SSC) published Payment Application Data Security Standard (PA-DSS) Version 3.1. Effective 1 June 2015, PA-DSS 3.1 aligns with the recent release of PCI Data Security Standard (PCI DSS) 3.1 primarily to address vulnerabilities in the Secure Sockets Layer (SSL) encryption protocol that can put payment data at risk. With this revision and supporting guidance, the Council urges organizations to understand if and how their payment applications are using SSL and upgrade to a secure version of Transport Layer Security (TLS).

The SSL protocol vulnerability primarily affects web servers and browsers. If exploited, it can jeopardize the security of any payment card data being accepted or processed. Upgrading payment applications and systems to a minimum of TLS 1.1 (the successor protocol to SSL) is the only known way to remediate SSL vulnerabilities that have been most recently exploited by browser attacks including POODLE and BEAST.

To address this risk, PA-DSS 3.1 updates requirements 8.2, 11.1 and 12.1-12.2 to remove SSL and early TLS[1] as examples of strong cryptography. PA-DSS 3.1 is effective on 1 June 2015, but there is a transition period for applications currently undergoing PA-DSS 3.0 validations:

- New application submissions to PA-DSS 3.0 will be accepted until 31 August 2015;
- Applications being validated against PA-DSS 3.0 which are “in queue” (that is, submitted with invoice paid) by 31 August 2015 will have until 30 November 2015 to complete the validation process;
- The expiry date for payment application listings validated to PA-DSS 3.1 is October 28, 2019.

The revision also includes other minor modifications to improve clarity based on stakeholder feedback.

The Council encourages organizations to use the following supporting resources in understanding PA-DSS 3.1 and its impact to security programs:

- **Summary of Changes from PA-DSS Version 3.0 to 3.1**: Highlights revisions made from version 3.0 to version 3.1.
- **PCI SSC Information Supplement: Migrating from SSL and Early TLS**: Provides guidance on use of interim risk mitigation approaches, migration recommendations and alternative options for strong cryptographic protocols, including FAQs and tips for small merchant environments.
- **FAQs for Transition from PA-DSS v3.0 to v3.1**: Answers to frequently asked questions about the validation process from PA-DSS v3.0 to v3.1.
- **Supporting Documents**: PA-DSS ROV Reporting Template, Attestation of Validation (AOV), and updates to the Frequently Asked Questions (FAQ) Knowledge Base.

PA-DSS 3.1 and supporting resources are available on the PCI SSC website at:
https://www.pcisecuritystandards.org/security_standards/documents.php

“The Council works closely with the payment security community on any changes made to the PCI Standards,” said PCI SSC Chief Technology Officer Troy Leach. “ This update falls in line with our mission of pushing for the best security as soon as possible, while empowering organizations to take a pragmatic, risk-based approach to protecting their data."

[1] TLS version 1.0 and in some cases 1.1 – see PCI SSC Information Supplement: Migrating from SSL and Early TLS.

About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Founded in 2006 by the major payment card brands American Express, Discover, JCB International, MasterCard and Visa Inc., the Council has 700 Participating Organizations representing merchants, banks, processors and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: pcisecuritystandards.org. Connect with the PCI Council on LinkedIn. Join the conversation on Twitter @PCISSC.

###