Media Contacts

Mark Meissner
PCI Security Standards Council
+1-202-744-8557
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 SECURITY STANDARDS COUNCIL PUBLISHES MINOR REVISION TO PCI DATA SECURITY STANDARD

—PCI DSS Version 3.2.1 Includes Minor Updates To Account for SSL/Early TLS Dates That Have Passed—

WAKEFIELD, Mass., 17 May 2018 — Today the PCI Security Standards Council (PCI SSC) published a minor revision to the PCI Data Security Standard (PCI DSS), which businesses around the world use to safeguard payment card data before, during and after a purchase is made. PCI DSS version 3.2.1 replaces version 3.2 to account for effective dates and Secure Socket Layer (SSL)/early Transport Layer Security (TLS) migration deadlines that have passed. No new requirements are added in PCI DSS v3.2.1. PCI DSS v3.2 remains valid through 31 December 2018 and will be retired as of 1 January 2019.

"This update is designed to eliminate any confusion around effective dates for PCI DSS requirements introduced in v3.2, as well as the migration dates for SSL/early TLS," said PCI SSC Chief Technology Officer Troy Leach. "It is critically important that organizations disable SSL/early TLS and upgrade to a secure alternative to safeguard their payment data."

The minor changes in PCI DSS v3.2.1 reflect how existing requirements are affected once the effective dates and SSL/TLS migration deadlines have passed so that organizations can accurately report how their implementations meet these existing requirements after 30 June. Specifically, the changes include:

- Removal of notes referring to an effective date of 1 February 2018 for applicable requirements, as this date has passed.
- Updates to applicable requirements and Appendix A2 to reflect that only POS POI (point of sale point of interaction) terminals and their service provider connection points may continue using SSL/early TLS as a security control after 30 June 2018.
- Removal of multi-factor authentication (MFA) from the compensating control example in Appendix B, as MFA is now required for all non-console administrative access; addition of one-time passwords as an alternative potential control for this scenario.

The updates in PCI DSS v3.2.1 do not affect the Payment Application Data Security Standard (PA-DSS), which will remain at v3.2.

PCI DSS v3.2.1 and a summary of changes from v3.2 to v3.2.1 are available now in the Document Library on the PCI SSC website. Updated versions of the Migrating from SSL and Early TLS Information Supplement, Self-Assessment Questionnaires (SAQ) and SAQ Instructions and Guidelines will be published shortly to support PCI DSS v3.2.1.

For more information, read PCI Perspectives blog Q&A with Chief Technology Officer Troy Leach: PCI DSS Now and Looking Ahead.

About the PCI Security Standards Council

The PCI Security Standards Council (PCI SSC) leads a global, cross-industry effort to increase payment security by providing industry-driven, flexible and effective data security standards and programs that help businesses detect, mitigate and prevent cyberattacks and breaches. Connect with the PCI SSC on LinkedIn. Join the conversation on Twitter @PCISSC. Subscribe to the PCI Perspectives Blog.

###