Payment Card Industry
Security Standards Council, LLC

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

Media Contacts

Laura K. Johnson Lindsay Goodspeed
PCI Security Standards Council
+1-781-876-6250
press@pcisecuritystandards.org
Twitter @PCISSC

PCI COUNCIL PUBLISHES REVISION TO PCI DATA SECURITY STANDARD

— PCI DSS 3.1 and supporting guidance helps organizations address vulnerabilities within SSL protocol that put payment data at risk; PA-DSS revision to follow —

WAKEFIELD, **Mass**., 15 April 2015 — Today, the PCI Security Standards Council (PCI SSC) published PCI Data Security Standard (PCI DSS) Version 3.1 and supporting guidance. The revision includes minor updates and clarifications, and addresses vulnerabilities within the Secure Sockets Layer (SSL) encryption protocol that can put payment data at risk. Available now on the PCI SSC website, version 3.1 is effective immediately. PCI DSS Version 3.0 will be retired on 30 June 2015.

The National Institute of Standards and Technology (NIST) identified SSL (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. Upgrading to a current, secure version of Transport Layer Security (TLS), the successor protocol to SSL, is the only known way to remediate these vulnerabilities, which have been exploited by browser attacks such as POODLE and BEAST.

To address this risk, PCI DSS 3.1 updates requirements 2.2.3, 2.3 and 4.1 to remove SSL and early[1] TLS as examples of strong cryptography. The revisions are effective immediately, but impacted requirements have a sunset date to allow for organizations with affected systems to implement the changes:

- SSL and early TLS cannot be used as security controls to protect payment data after 30 June 2016.
- Prior to this date, existing[2] implementations that use SSL and/or early TLS must have a formal risk mitigation and migration plan in place. Guidance on interim risk mitigation approaches, migration recommendations and alternative options for strong cryptographic protocols is outlined in the PCI SSC Information Supplement: Migrating from SSL and Early TLS.
- Effective immediately, new[3] implementations must not use SSL or early TLS.
- Point-of-sale (POS)/Point-of-interaction (POI) terminals (devices such as magnetic card readers or chip card readers that enable a consumer to make a purchase) that can be verified as not being susceptible to all known exploits for SSL and early TLS may continue using these protocols as a security control after 30 June 2016.

“We are focused on providing the strongest standards and resources to help merchants and their business partners protect against the latest threats to payment data. The PCI Standards development process allows us to do this based on industry and market input,” said PCI SSC General Manager Stephen W. Orfei. “With PCI DSS 3.1 and supporting guidance we are arming organizations with a pragmatic, risk-based approach to addressing the vulnerabilities within the SSL protocol that can put payment data at risk.”

Additional changes to improve understanding and consistency in the standard include: clarification of language, general formatting and typographical corrections; additional guidance in introductory sections and guidance column; and updates to specific testing procedures to align testing objectives with requirements.

---

[1] TLS version 1.0 and in some cases 1.1 – see PCI SSC Information Supplement: Migrating from SSL and Early TLS.
[2] Existing implementations are those where there is a pre-existing reliance or use of a vulnerable protocol(s) – see PCI SSC Information Supplement: Migrating from SSL and Early TLS.

[3] 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.

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

- **Summary of Changes from PCI 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
- **Understanding PCI DSS Version 3.1** – an on-demand webinar outlining the revisions and guidance, available here
- **Supporting documents** - Self-Assessment Questionnaires (SAQ); Attestations of Compliance (AOC); Report on Compliance (ROC) Template; PCI DSS Glossary of Terms, Abbreviations, and Acronyms; and updates to the Frequently Asked Questions (FAQ) Knowledge Base will be published shortly

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

Supporting this revision, Payment Application Data Security Standard (PA-DSS) Version 3.1 will also be published shortly.

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: www.pcisecuritystandards.org.
Connect with the PCI Council on LinkedIn. Join the conversation on Twitter @PCISSC.

###