PCI Security Standards Council

Payment Card Industry
Security Standards Council, LLC

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

Media Contact

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

PCI SECURITY STANDARDS COUNCIL REVISES DATE FOR MIGRATING OFF VULNERABLE SSL AND EARLY TLS ENCRYPTION

— Organizations Using SSL and Early TLS Encryption are Vulnerable to Attack and Must Change to a secure version of TLS (currently 1.1 or Higher) by June 2018 —

WAKEFIELD, Mass., 18 December 2015 — Following significant feedback from the global PCI community and security experts, the Payment Card Industry Security Standards Council (PCI SSC), a global forum for the development of payment card security standards, today announced a change to the date that organizations who process payments must migrate to TLS 1.1 encryption or higher. The previous date of June 2016 has been moved to June 2018.

The original deadline date for migration, June 2016, was included in the most recent version of the PCI Data Security Standard, version 3.1 (PCI DSS 3.1), which was published in April of 2015. The new deadline date, June 2018, will be included in the next version of the PCI Data Security Standard, which is expected in 2016.

“Early market feedback told us migration to more secure encryption would be technically simple, and it was, but in the field a lot of business issues surfaced as we continued dialog with merchants, payment processors and banks,” said Stephen Orfei, General Manager, PCI SSC. “We want merchants protected against data theft but not at the expense of turning away business, so we changed the date. The global payments ecosystem is complex, especially when you think about how much more business is done today on mobile devices around the world. If you put mobile requirements together with encryption, the SHA-1 browser upgrade and EMV in the US, that’s a lot to handle. And it means it will take some time to get everyone up to speed. We’re working very hard with representatives from every part of the ecosystem to make sure it happens as before the bad guys break in.”

“Some payment security organizations service thousands of international customers all of whom use different SSL and TLS configurations,” said Troy Leach, Chief Technology Officer, PCI SSC. “The migration date will be changed in the updated Standard next year to accommodate those companies and their clients. Other related provisions will also change to ensure all new customers are outfitted with the most secure encryption into the future. Still, we encourage all organizations to migrate as soon as possible and remain vigilant. Staying current with software patches remains an important piece of the security puzzle.”

—more—

In addition to the migration deadline date-change, the PCI Security Standards Council has updated:

- A new requirement date for **payment service providers** to begin offering more secure TLS 1.1 or higher encryption
- A requirement for **new implementations** to be based on TLS 1.1 or higher
- An **exception to the deadline** date for Payment Terminals, known as “POI” or Points of Interaction.

To answer questions about the migration deadline date-change and other requirement updates, the PCI Security Standards Council has recorded a webinar that includes the National Institute of Standards and Technology (NIST), which originally reported the vulnerabilities in SSL and early versions of TLS in 2014. Expert speakers from the Assessor community, who review and grade organizations on compliance with payment security requirements, are also on the webcast.

In addition, a Bulletin on Migration has been created and is available for download from the PCI Security Standards Council website.

Merchants are encouraged to contact their payment processors and / or acquiring banks for detailed guidance on upgrading their ecommerce sites to the more secure encryption offered by TLS 1.1 or higher.

About the PCI Security Standards Council

The PCI Security Standards Council is a 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 Financial Services, JCB International, MasterCard Worldwide and Visa Inc., the Council has over 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: http://pcisecuritystandards.org.

Connect with the PCI Council on LinkedIn: http://www.linkedin.com/company/pci-security-standards-council

Join the conversation on Twitter: http://twitter.com/#!/PCISSC

###