Media Contacts

Laura K. Johnson, Ella Nevill
PCI Security Standards Council
+1-781-876-6250
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 UPDATES STANDARD FOR PIN TRANSACTION SECURITY

— Updates provide robust criteria for payment acceptance device vendors and testing labs —

WAKEFIELD, Mass., 07 June 2013 — Today the PCI Security Standards Council (PCI SSC), an open, global forum for the development of payment card security standards published version 4.0 of the PIN Transaction Security (PTS) Point of Interaction (POI) requirements. These requirements, along with the Hardware Security Module (HSM) requirements provide standards for device manufacturers to ensure merchants and others have secure devices for accepting and processing payment cards.

Point of Interaction (POI) devices, such as PIN entry devices, continue to be a primary method for accepting and processing credit payment cards and a target for criminal attack. As part of its ongoing standards development process, the PCI Council makes updates based on industry needs and changing threats, to ensure the strongest technical standards for payment security.

Changes introduced in version 4.0 of the PTS POI requirements focus on increasing the robustness of the devices through enhanced testing procedures and streamlining the evaluation and reporting processes for both device vendors and testing labs.

The PTS POI requirements are updated on a three-year cycle, based on feedback from the PCI community. The development process also allows for minor update releases as needed – in October 2011, for example, the Council issued version 3.1 to support deployment of point-to-point encryption (P2PE) and mobile technologies. The new version builds on these updates to underscore the requirements' applicability to traditional POI deployments – including Point-of-Sale devices, unattended kiosks, mobile dongles – and many other types of devices.

Key changes include:

- **Restructured Open Protocols Module** – helps ensure POI devices do not have communication vulnerabilities that can be remotely exploited to gain access to sensitive data or resources within the device

- **Enhanced interface testing and logical security requirements** – by requiring more stringent documentation and assessment of all interfaces of the device, will help ensure that no interface can be abused or used as an attack vector

- **Added source code reviews** – additional mandatory source code reviews enhance the robustness of the testing process

- **Introduction of a vendor provided security policy** – provides guidance that will facilitate implementation of an approved POI device in a manner consistent with the POI requirements, including information on key management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements

The requirements are available on the PCI SSC website at: https://www.pcisecuritystandards.org/security_standards/documents.php. For ease of reference, a summary of changes from version 3.1 to version 4.0 are included with the requirements update.

The Council will also be hosting a webinar on the updated requirements on 18 and 20 June. For more information and to register, visit: https://www.pcisecuritystandards.org/training/webinars.php.

“The PTS POI requirements are critical to securing POI devices,” said Bob Russo, general manager, PCI Security Standards Council. “By continually enhancing the robustness of the program’s testing criteria we can ensure that these products are being tested and validated against the highest level of security.”

Vendors now have the option of testing against version 3.1 or version 4.0. Beginning in May 2014 version 3.0 will no longer be available for new evaluations, but may still be used for delta evaluations.

“With 3.1 we introduced changes that would help facilitate the use of point-to-point encryption technology and open platforms, such as mobile phones, to accept payments,” said Troy Leach, chief technology officer, PCI Security Standards Council. “Version 4.0 continues to build on this by addressing all interfaces that potentially grant access to data or resources in POI devices, in addition to the critical communications channels, such as RFID, wireless, cellular (e.g. GPRS, CDMA) and Bluetooth.”

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 Financial Services, JCB International, MasterCard Worldwide and Visa Inc., the Council has more than 650 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: http://www.linkedin.com/company/pci-security-standards-council

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