Media Contacts

Laura K. Johnson
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 PUBLISHES TERMINAL SOFTWARE SECURITY BEST PRACTICES

— Resource arms software developers with best practices to ensure they deliver secure code —

Wakefield, MA., 16 December 2014 – Today the PCI Security Standards Council, an open global forum for the development of payment card security standards, published the *Terminal Software Security Best Practices*. The document gives detailed guidance on the secure development of software designed to run on point-of-interaction devices.

Point-of-interaction (POI) devices continue to be highly targeted by criminals. PCI PIN Transaction Security (PTS) requirements address software code required to meet parameters defined in the PCI PTS POI Security Requirements. *Terminal Software Security Best Practices* is intended to address other software that exists on the POI device, including both payment and non-payment applications, and reinforces the importance of maintaining a layered approach to security. As fraud continues to evolve, it is important that efforts are made to ensure that all code within the payment ecosystems is secure.

This new guidance will help organizations including POI device vendors that write or implement applications within a POI device, understand the potential threats, and employ appropriate processes throughout the development life cycle to counter those threats. Organizations can use this guidance to help ensure standard secure coding practices are followed, including:

Security awareness training that supports secure software development:

- Those involved in the development process (including software developers and peer reviewers), have important roles to play in developing software to ensure secure coding practices are implemented and address current threats. Those roles need to be defined before development begins and those individuals need to be trained and understand the secure software development program.

Secure software development lifecycle:

- Organizations need to have a software security roadmap defined before development begins that will address known threats. The software needs to be mapped and

documented, and rules and processes defined so that security is implemented as part of the development process and not incorporated as an afterthought.

Device level testing:

- It is imperative to understand how the application will work when used with the hardware, firmware, and other applications that it is intended for use with. While simulators and unit testing are essential, testing the device with the complete solution should be a priority.

Internal process reviews:

- The threat environment is constantly evolving which is why organizations need to stay current on the latest threats and changes to ensure the procedures in place are still sufficient and are actually being followed.

The *Terminal Software Security Best Practices* information supplement is available for download on the PCI SSC website.

"Criminals are looking at every aspect of a payment transaction to find ways for data exfiltration," said PCI SSC Chief Technology Officer, Troy Leach. "While consumers and merchants alike benefit from additional features, complexity and increasing dependency on third-party applications can create new opportunities for exploit which is why due diligence is so vital in the development of software that terminals rely upon. This paper highlights important best practices for software coding in this unique environment."

As with all PCI Council information supplements, the guidance provided in this document is supplemental and does not supersede or replace any PCI DSS requirements.

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 more than 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: http://www.linkedin.com/company/pci-security-standards-council. Join the conversation on Twitter: http://twitter.com/#!/PCISSC

###