PCI COMPLIANCE 2.0

TAMPA OWASP

Kathleen Ann Mullin, CIA, CISA, CISSP, CISM, CRSIC, CGEIT

September 13, 2011

Mandatory Credit Card Security Programs

No the sky is not falling!

https://www.pcisecuritystandards.org

Requirement 6: Develop and maintain secure systems and applications

6.5 Develop applications based on secure coding guidelines.

As industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.

New Stuff

Prevent common coding vulnerabilities in software development processes, to include the following:

6.5.6 All “High” vulnerabilities identified in the vulnerability identification process.

Note: *This requirement is considered a best practice until June 30, 2012, after which it becomes a requirement.*

It's not just applications anymore

- Any high vulnerabilities that could affect the application should be accounted for during the development phase.
- For example, a vulnerability identified in a shared library or in the underlying operating system should be evaluated and addressed prior to the application being released to production.

Risk Ranking

6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.

Notes:

♣ *Risk rankings should be based on industry best practices. For example, criteria for ranking "High" risk vulnerabilities may include a CVSS base score of 4.0 or above, and/or a vendor-supplied patch classified by the vendor as "critical," and/or a vulnerability affecting a critical system component.*

♣ *The ranking of vulnerabilities as defined in 6.2.a is considered a best practice* ***until June 30, 2012, after which it becomes a requirement****.*

http://www.us-cert.gov/cas/bulletins/

http://www.first.org/cvss/cvss-guide.html

cvss

Due Care Does Not Mean Secure

Questions

??
??
??
??
??
??
??
??
??
??
??
??
??
??
??
??
???

Thanks

kathleen.mullin@yahoo.com