blackfoot Newsflash

SSL and TLS Vulnerabilities and PCI compliance

On Wednesday 15th April 2015, the PCI Security Standards Council published an update to the PCI Data Security Standard (PCI DSS). A significant update was applied to the standard in relation to Section 2.2.3. The update is regarding the numerous recent security vulnerabilities associated with SSL and TLS which are encryption protocols used to protect communications: typically encrypting payments on web sites.

The update is significant for merchants who must comply with PCI DSS as it mandates that, effective immediately, any new implementation of a payment system must not use SSL or early versions of TLS (less than V1.2). It also specifies that existing implementations must have immediate risk mitigation and migration plans in place for an update no later than June 30th 2016.

What is the threat

The reason the PCI SSC has mandated this change is that the security vulnerabilities in SSL and early versions of TLS could be used by attackers to compromise encrypted communications.

What is the potential impact

Attackers can compromise sensitive information, which may include payment card details. Affected organisations risk losing their PCI compliance status and potential fines.

How to tell if you are affected or vulnerable

There are two ways to determine if your website is vulnerable:

- Instigate a remote scan of the service to identify which proposed encryption algorithms are in use, or
- Check the configuration of the web server to identify which protocols are supported.

If the algorithms supported are SSL or a TLS version less than V1.2 then the website is vulnerable. Please refer to the advice in the following section for advice on the recommended next steps.

What to do next

For all systems in PCI scope, verify whether SSL or early versions of TLS are is use – for those that are affected, produce a risk mitigation and migration plan which ensures compliance by the 30th June 2016. Update all server build standards to ensure compliance with the new PCI DSS V3.1 requirements.

Blackfoot statement of opinion

Previously the PCI SSC has followed a documented 3 year standard lifecycle with a number of structured phases involved in reviewing, retiring, feedback, revisions and final review. This lifecycle enabled organisations to plan changes to applications, environments, processes and outsource partners over a budgetary cycle - in good time not to interfere with late stage projects and current application development. The retirement of PCI DSS V3.0 after only 6 months and the instant application of the SSL/early TLS changes are a break in this protocol and will have a large impact for many organisations, with issues such as temporarily halting late stage projects whilst these changes are implemented prior to go live. This may add both delays and costs to late stage 'pre-budgeted' projects and in parts of the world where PCI DSS is law may leave some organisations at risk of legal breach.

This new precedent may herald the introduction of shorter notice or grace periods.

Further reading

PCI DSS V3.1: https://www.pcisecuritystandards.org/security_standards/index.php

Microsoft IIS: https://support.microsoft.com/en-us/kb/187498

Apache: http://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslprotocol

Nginx: http://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_protocols

Tomcat: https://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html#Edit_the_Tomcat_Configuration_File

Getting in touch

Should you require any further support please contact your Blackfoot representative, call 0845 805 2409 or email info@blackfootuk.com

blackfoot

BLACKFOOT UK LIMITED
Tel: 0845 805 2409 E-mail: info@blackfootuk.com
Web: www.blackfootuk.com