SSL / Early TLS migration plan

⚠ The below document is now defunct. All TLS 1.0 must be disabled now.

Overview

Risk Mitigation and Migration Plan for Payment Card Industry Data Security Standard (PCI DSS) 3.1 Requirements

PCI SSC has released version 3.1 of the PCI DSS requirements. A key part of these new requirements mandates that SSL (Secure Socket Layers) and early versions of TLS (Transport Layer Security) no longer be used for web servers.

Due to the number of web browsers not fully supporting TLSv1.1, we plan to delay our full migration to TLSv1.1/1.2 by 30th June 2018.

A description of where and how we are currently using SSL and/or early versions of TLS, how we intend to mitigate the risks with these technologies, and our migration plan are listed below.

Plan

Where is SSL/TLS 1.0 currently used?

SSL/TLS 1.0 usage has now been limited to customers using older browsers on the front end website at https://secure.gemporia.com and https://secure.gemcollector.com

The affected browsers are listed below:

- Firefox before version 27
- Chrome before version 22
- Internet Explorer before version 11
- Opera before version 14
- Safari before version 7
- Android before version 4.4

No payment data is transmitted over Gemporia's sites running TLS 1.0. Only customer personal data such as name, address and order details are transmitted. Payment details are sent via the hosted payment pages on Adyen, PayPal and Barclaycard.

How are we mitigating risks with SSL/TLS 1.0?

By specifying a preference for cipher order we are able to ensure that clients who can support more secure protocols do always use them.

How are we monitoring for new vulnerabilities associated with SSL/TLS 1.0?

We monitor the National Vulnerability Database for all new CVE's associated with SSL/TLS 1.0, and work with an independent 3rd party (Security Metrics) to verify that our systems are up-to-date and secure.

How are we ensuring that new SSL/TLS 1.0 systems are not introduced into the cardholder data environment?

The Configuration Standards document has been updated to require tools are used on new servers to permit only allowed protocols

When will the migration plan from SSL/TLS1.0 be completed?

TLS 1.0 will be disabled on our front end website on June 30th 2018 and customers who have not upgraded their web browsers by then will no longer be able to access our services.

How to Review

The position on using early TLS is dictated by the volume of traffic received from Android devices lower than version 4.4. This is the only pool of people who have no other option for browsing our site. As a result the percentage must drop below an acceptable level to allow early migration from TLS1.0. This is to be discussed with the Digital Marketing team and Website Manager.

Revision History

Date	Description	Who
12/08/2015	Original Document	Andrew Smith
01/11/2016	Updated date to new target date	Andrew Smith
05/10/2016	Migrated to wiki, no change	Andrew Smith
03/11/2016	Expanded to new format as per Appendix A2 of PCI DSS Spec	Andrew Smith
06/11/2016	Added “How to Review” section	Andrew Smith
04/01/2017	Reviewed, no change	Andrew Smith
04/04/2017	Reviewed, no change	Andrew Smith
04/07/2017	Reviewed, no change	Andrew Smith