Tech Tip Tuesday—March 28, 2017

IMPORTANT NOTICE REGARDING CREDIT CARD GATEWAY (PAYFLOWPRO)

Back in February, we had a Tech Tip regarding announcements from DEEM regarding upgrading their security standards to something known as “TLS 1.2”.

Now PayPal is upgrading their security standards for the same reasons, effective June 2017.

In order to be fully compatible with the security standard, the windows operating system on any machine on which you process credit cards (preauthorizations, deposits, or TripBook) must have a Windows component called “.net framework 4.5” installed on the machine. Typically, this is handled through the Windows update process.

However, the 4.5 framework will only work on workstations running Windows 7 or higher, or servers running Server 2008 or higher.

You can test whether your workstation is compatible with TLS 1.2 by opening a web browser and going to the address https://www.howsmyssl.com/ Screen shots of both “good” and “bad” are at the end of this note.

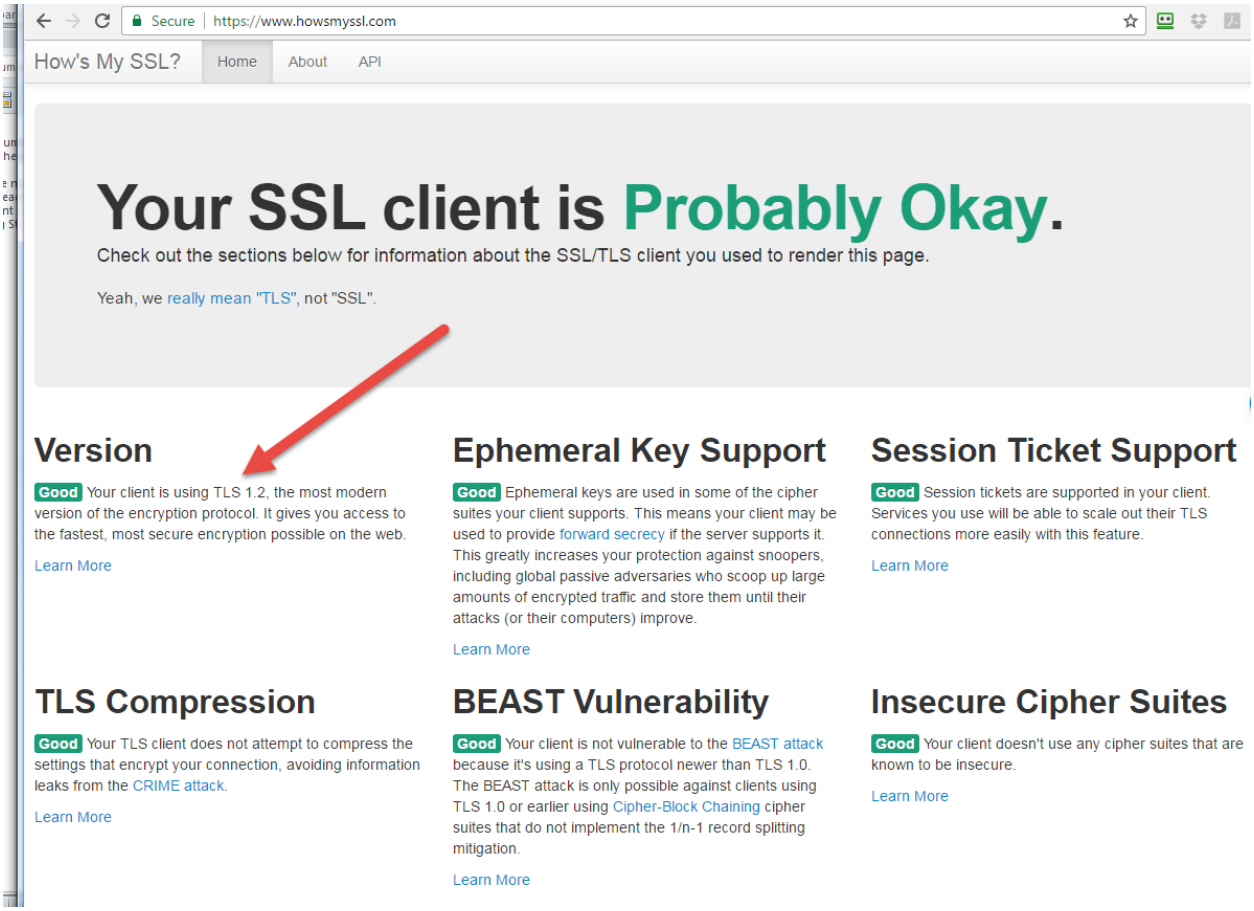
If you are running Livery Coach on a Windows XP machine, this means you will not be able to process credit card transactions.

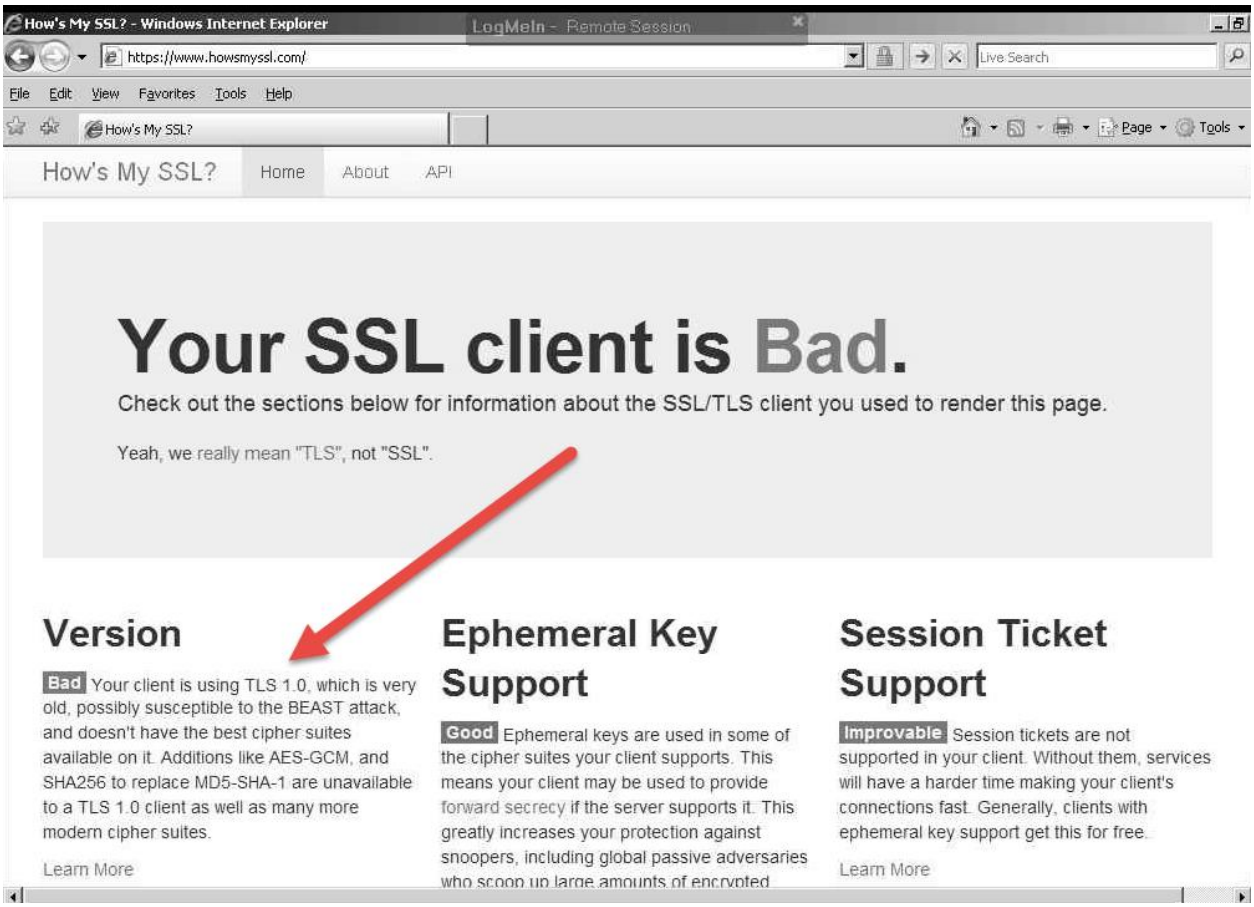
Furthermore, if you are still running the “old” version of Livery Coach, you will not be able to process credit cards. You must be running LiveryCoach.net. Remember we have added hundreds of new features and functions to LiveryCoach.net, while we stopped updating the “old” version of Livery Coach in 2014. If you have not completed your transition, now you have a deadline!

For assistance or questions, please reach out to our support team.

Windows XP was introduced in 2002, and Microsoft ended all support (including security updates) in April 2014. Server 2003 support ended in July 2015.

Thank you for your cooperation.


Secure | https://www.howsmyssl.com
How's My SSL?
Home
About
API
Your SSL client is Probably Okay.
Check out the sections below for information about the SSL/TLS client you used to render this page.
Yeah, we really mean "TLS", not "SSL".
Version
Good Your client is using TLS 1.2, the most modern version of the encryption protocol. It gives you access to the fastest, most secure encryption possible on the web.
Learn More
Ephemeral Key Support
Good Ephemeral keys are used in some of the cipher suites your client supports. This means your client may be used to provide forward secrecy if the server supports it. This greatly increases your protection against snoopers, including global passive adversaries who scoop up large amounts of encrypted traffic and store them until their attacks (or their computers) improve.
Learn More
Session Ticket Support
Good Session tickets are supported in your client. Services you use will be able to scale out their TLS connections more easily with this feature.
Learn More
TLS Compression
Good Your TLS client does not attempt to compress the settings that encrypt your connection, avoiding information leaks from the CRIME attack.
Learn More
BEAST Vulnerability
Good Your client is not vulnerable to the BEAST attack because it's using a TLS protocol newer than TLS 1.0. The BEAST attack is only possible against clients using TLS 1.0 or earlier using Cipher-Block Chaining cipher suites that do not implement the 1/n-1 record splitting mitigation.
Learn More
Insecure Cipher Suites
Good Your client doesn't use any cipher suites that are known to be insecure.
Learn More


How's My SSL? - Windows Internet Explorer
LogMeIn - Remote Session
https://www.howsmyssl.com/
Live Search
File Edit View Favorites Tools Help
How's My SSL?
Page Tools
How's My SSL?
Home
About
API
Your SSL client is Bad.
Check out the sections below for information about the SSL/TLS client you used to render this page.
Yeah, we really mean "TLS", not "SSL".
Version
Bad Your client is using TLS 1.0, which is very old, possibly susceptible to the BEAST attack, and doesn't have the best cipher suites available on it. Additions like AES-GCM, and SHA256 to replace MD5-SHA-1 are unavailable to a TLS 1.0 client as well as many more modern cipher suites.
Learn More
Ephemeral Key Support
Good Ephemeral keys are used in some of the cipher suites your client supports. This means your client may be used to provide forward secrecy if the server supports it. This greatly increases your protection against snoopers, including global passive adversaries who scoop up large amounts of encrypted
Session Ticket Support
Improvable Session tickets are not supported in your client. Without them, services will have a harder time making your client's connections fast. Generally, clients with ephemeral key support get this for free.
Learn More