Security Update
18th September 2015

eCorner®

End support for SSL V1, V2, V3 and TLS V1.0

Security Update Overview

There are many potential threats to your online business. Many of these threats are caused by hackers and malicious software.

eCorner employs a range of security methods to stop information being stolen or changed in your website. There is the physical security in our data center and there are also systems and software that make your websites secure.

Systems and software must be regularly updated to keep ahead of the hacker and malware they use.

To protect your business and personal information eCorner must remove older security systems from our servers and install the latest version just like you should update anti-virus software on your own business and personal computers.

This security upgrade will have an impact on visitors accessing your website if they do not use a computer and web browser that is up to date with the security patches and software releases recommended by suppliers like Microsoft and Apple.

eCorner will, at a minimum, support the security protocol called **Transport Layer Security Version 1.1** (TLS 1.1). This change will occur from January 2016.

Action required summary:

1. Ensure that the computer and browser that you use to access your website and administration is up to date.
2. Update the terms and conditions / privacy policy on your website.
3. Notify regular customers that some older browsers are no longer secure.
4. Add a note in the checkout process first step explaining that older and unsecure browsers are no longer supported and that a customer using those may not be able to complete checkout.

Information is available in the remainder of this document that details the changes and actions needed.

What action do we need to take?

In order to maintain seamless access to your website and administration, you need to ensure that browsers connecting to your website have **TLS 1.1 encryption or higher enabled which you can find – click here**.

If your browser (or any custom integration) does not have TLS 1.1 or higher enabled after we make this change, then **your customers and administrators will NOT be able to complete orders on your website or access secure pages**.

We recommend that you begin planning to support TLS 1.1 and TLS 1.2 as soon as possible.

You will need to communicate to your customers that they will have to make changes to the browser that they use to access your website. This security change is not just impacting your website or even just eCorner customers, it is a broad change that will impact all websites worldwide during 2016.

When will eCorner disable TLS 1.0 encryption?

eCorner plans to disable TLS 1.0 encryption beginning **from January 2016**.

Enabling TLS 1.1 and 1.2 in Internet Explorer

Online store and website owners who want to continue using Internet Explorer 8, 9, and 10 to access secure pages (such as the administration area and storefront checkout pages) can do this by making some changes to their Internet Explorer browser settings. This information should also be communicated to your customers via an information article or note on your website.

1. On the Internet **Explorer main menu**, select **Tools > Internet Options**.
2. In the Internet Options box, select the **Advanced tab**.
3. In the Security category,
    - Uncheck - Use SSL 3.0 and
    - **Check - Use TLS 1.0, Use TLS 1.1, and Use TLS 1.2** (if available).
4. Click OK
5. Exit and restart Internet Explorer.

Note it is important to check consecutive versions. Not selecting consecutive versions (e.g. checking TLS 1.0 and 1.2, but not checking 1.1) could result in connection errors.

A full list of browsers and compatibility can be found further down in this document.

We recommend that you notify your customers of these changes.

Informing your customers well in advance will help you avoid any loss of business and minimise questions. It is recommended at that you add some information to your Terms & Conditions and / or Privacy Policy pages on your website. You have our approval to use any content in this communication. You might also consider adding the information to a newsletter if your send those to regular customers.

This information is available on our website at - www.ecorner.com.au/security-notification-ssl-tls-2016.

What is the security change?

Starting in **January 2016**, eCorner will be disabling the **TLS 1.0** encryption protocols; **SSL V1, SSL V2 and SSL V3** have already been disabled. The process will be completed by the 31st January 2016 and at the time the minimum level of encryption protocol supported will be TLS 1.1. This will prevent the disabled protocols from being used to access secure pages of your website and administration for inbound and outbound connections.

What are SSL and TLS Encryption Protocol

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as 'SSL', are cryptographic protocols designed to provide communications security over a computer network. These are used to stop malicious access to secure information on your website such as credit card information or customer data.

You can find more information at Wikipedia.

Why is this happening?

To maintain the highest security standards and promote the safety of your data, we occasionally need to make security improvements and retire older encryption protocols. To maintain alignment with these best practices and updated compliance requirements from the **Payment Card Industry (PCI) Security Standards Council**, eCorner will disable the use of TLS 1.0 for connections to and from all customer websites.

You can find more information at the PCI Council website – PCI DSS V3.1 and SSL.

How do you know if you are ready for this change?

After we disable SSL V1, SSL V2, SSL V3 and TLS 1.0, any inbound connections to or outbound connections will need to use the TLS 1.1 or TLS 1.2 encryption protocol. This change impacts all customer websites. Three different areas require encryption to access your website:

- Internet browser,
- Custom API (inbound) integrations and
- Custom call-out (outbound) integrations.

An overview of each follows:

Internet Browsers:

You and your users should not experience an impact accessing your website in your browser(s) unless you are using a non-supported browser or you have disabled the supported encryption protocols in the browser. Please refer to the compatibility guidelines below:

Browser	**TLS 1.1 or Higher Compatibility Notes**
Microsoft Internet Explorer (IE)	Review the information at the section on enabling TLS 1.1 and 1.2 – please note that compatibility will vary based on the version
Desktop and mobile IE version 11	Compatible by default for website front end but not administration
Desktop IE versions 9 and 10	Capable for website front end but not administration when run in Windows 7 or newer, but not by default. Review the information at the section on enabling TLS 1.1 and 1.2
Desktop IE versions 8 and below	Capable for website front end but not administration when run in Windows 7 or newer, but not by default. Review the information at the section on enabling TLS 1.1 and 1.2
Mobile IE versions 10 and below	Not compatible with TLS 1.1 or higher encryption.
Microsoft Edge	**Compatible by default**
Mozilla Firefox	**Compatible with the most recent, stable version, regardless of operating system**
Firefox 27 and higher	Compatible by default
Firefox 23 to 26	Capable, but not by default.
Firefox 22 and below	Not compatible with TLS 1.1 or higher encryption.
Google Chrome	**Compatible with the most recent, stable version, regardless of operating system**
Google Chrome 38 and higher	Compatible by default
Google Chrome 22 to 37	Capable for website front end but not administration when run in Windows XP SP3, Vista, or newer (desktop), OS X 10.6 (Snow Leopard) or newer (desktop), or Android 2.3 (Gingerbread) or newer (mobile)

Browser	TLS 1.1 or Higher Compatibility Notes
Google Chrome 21 and below	Not compatible with TLS 1.1 or higher encryption.
Google Android OS Browser	
Android 5.0 (Lollipop) and higher	Compatible by default
Android 4.4 (KitKat) to 4.4.4	Capable for website front end but not administration, but not by default.
Android 4.3 (Jelly Bean) and below	Not compatible with TLS 1.1 or higher encryption.
Apple Safari	
Desktop Safari versions 7 and higher for OS X 10.9 (Mavericks) and higher	Compatible by default
Desktop Safari versions 6 and below for OS X 10.8 (Mountain Lion) and below	Not compatible with TLS 1.1 or higher encryption.
Mobile Safari versions 5 and higher for iOS 5 and higher	Compatible by default
Mobile Safari for iOS 4 and below	Not compatible with TLS 1.1 or higher encryption.

Custom API (inbound) Integrations:

API Integrations are interfaces or applications that are separate from ePages, but use website data. If you have any API Integrations that you have enabled outside of eCorner and ePages, please ensure that the TLS 1.1 and/or TLS 1.2 encryption protocols are enabled in those integrations.

API integrations that use Java will generally need to use Java 8 or higher to enable TLS 1.1 and TLS 1.2 in call-outs by default. Another option is to use Java 7 and enable TLS 1.1 and/or TLS 1.2 using the https.protocols Java system property, if applicable, and/or source code changes to enable TLS 1.1 and TLS 1.2 on SSLSocket and SSLEngine instances.

Services that run on Windows Server systems and use Microsoft Secure Channel for TLS will need to run on Windows Server 2008 R2 or higher. This generally includes most .NET applications and Microsoft Internet Information Server (IIS). Earlier versions of Windows Server do not support TLS 1.1 or TLS 1.2.

Custom Call-out (outbound) Integrations:

Call-outs are integrations where your website refers to an outside source to either verify login credentials, push data, or pull data. If you use call-out integrations that have not been provided by eCorner or ePages please ensure that TLS 1.1 and/or TLS 1.2 are enabled in those integrations.