Shift Security Advisory 17 October 2011

Audience: Non-Technical Users. For a complete technical advisory, please contact info@shiftsys.com

Recently, researchers at the Ekoparty conference held in Buenos Aires credibly demonstrated a mechanism to untraceably decrypt and control connections protected by SSL v3.0 and TLS v1.0 protocols. These versions of the protocols and even less secure earlier versions are the predominant methods employed by most web servers and web browsers to encrypt and authenticate Internet communications. Because of this vulnerability and the proven exploit demonstrated by the researchers, it is advisable to take steps to limit the ability for an outside attacker to intercept and decrypt privileged communications.

The only widely used browser capable of employing the more secure TLS 1.1 or 1.2 protocol is Internet Explorer 8 or above on Windows Vista, Service Pack 1 or Windows 7. All other browsers, including Firefox, Safari on the Mac OS, and Chrome are, as of this writing, still vulnerable to the exploit. In addition, other services, e.g. email (IMAP, POP) that have connections secured by SSL may also be exposed to this exploit.

To configure Internet Explorer 8, click the gear icon in the top right corner, and select “Internet Options”. When the “Internet Options” dialogue is presented, select the “Advanced” tab. Scroll to the bottom of the checkmark list under “Security” and ensure that the following are DESELECTED:

- “Use SSL 2.0”
- “Use SSL 3.0”
- “Use TLS 1.0”

Ensure that the following are SELECTED:

- “Use TLS 1.1”
- “Use TLS 1.2”

Once confirmed, click “OK” and close the browser.

This may result in many websites that have not had their web servers upgraded to the TLS 1.1 or TLS 1.2 protocols failing to resolve. If this is the case, Internet Explorer will display a page that says “Internet Explorer cannot display the webpage”. This tells you the website you are visiting is using the compromised version of the SSL or TLS protocols. To use this website, you will need to reselect the appropriate protocol in the Internet Options page, but be aware that the connection may be surreptitiously intercepted and decrypted.