

IMMEDIATE ATTENTION Web Security Risk – 10/20/14 from Chestnut Health Systems

There was an announcement this week of a major security risk being dubbed, poodle. Because of this risk, we need all users who connect to any of our secure systems to upgrade their browsers and make the necessary changes listed below to make sure that your data being entered is protected. This is a risk for all secure systems on the internet, so it is highly recommended that you do this anyway, but required that these actions be done in order to connect with any of the systems we host. **I would highly recommend that you do this for your work and home computers!!**

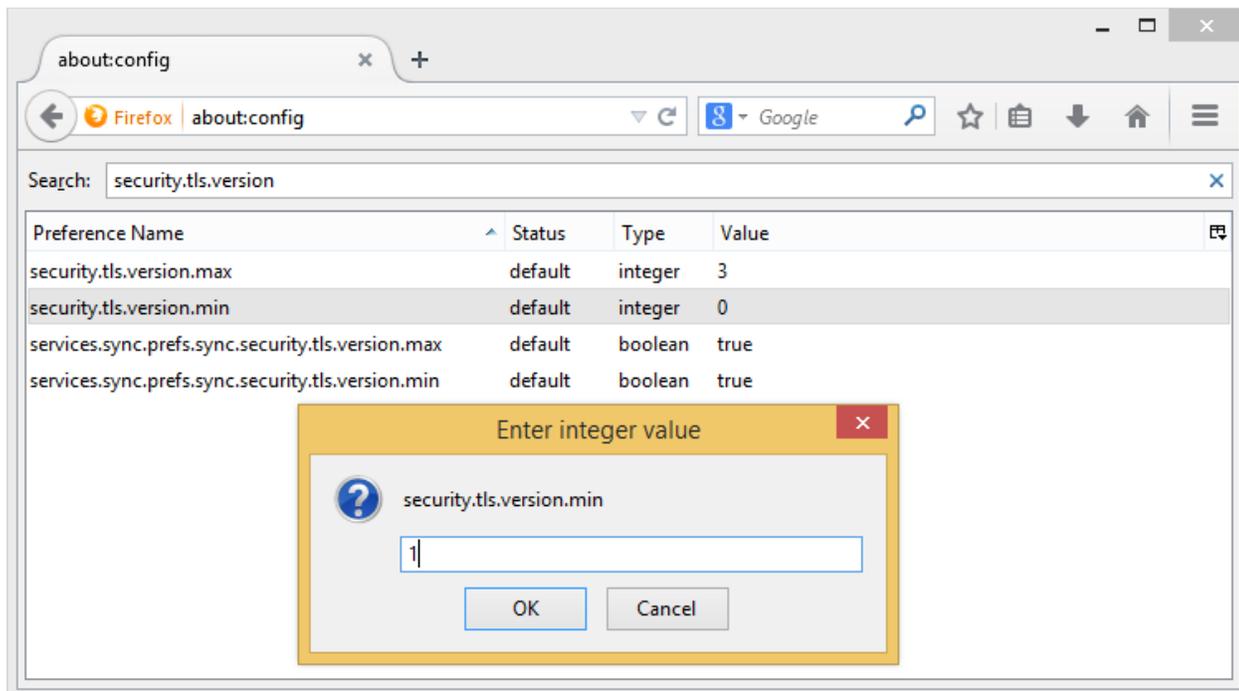
FIRST, you must have a current version of your browser installed. All of the major browsers offer free upgrades of their browsers and it only takes a couple of minutes to upgrade.

- We require users of Internet Explorer (IE) to be using at least version 8.0.
- We require users of Mozilla FireFox to be using at least version 30.0
- We require users of Google Chrome version 38
- Because of this issue, we cannot currently support use of our systems on Apple's Safari browser or any native mobile browser. If you are working on a Mac or a tablet, please install either FireFox or Chrome and follow directions below.

SECOND, Client browsers must do the following:

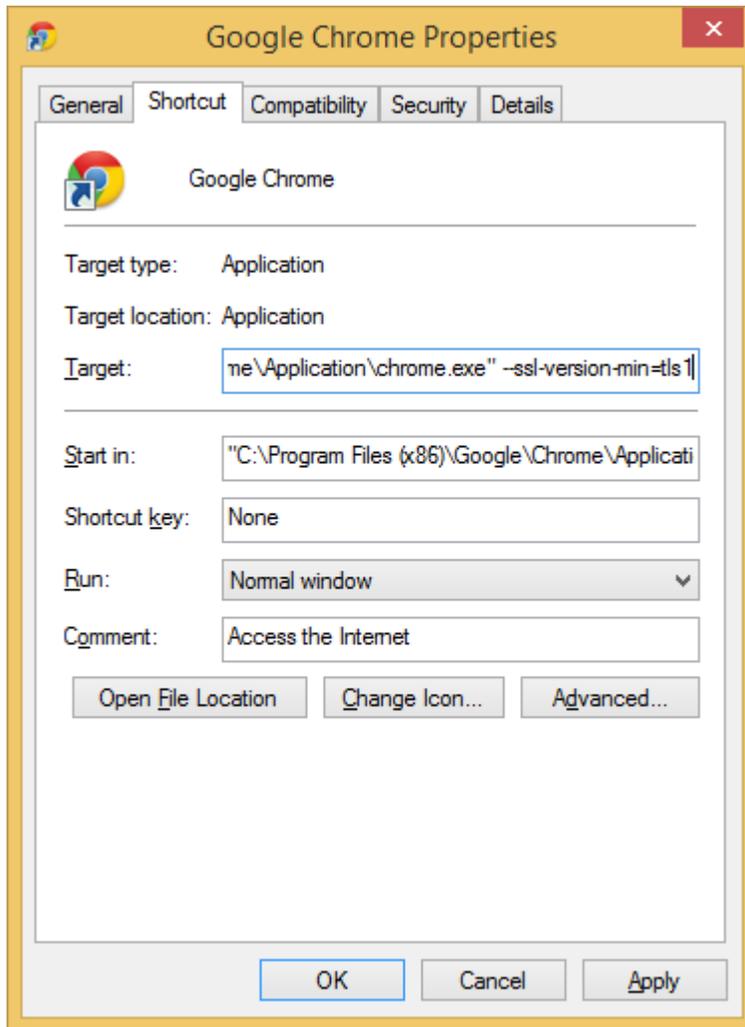
***Firefox – will be automatically implemented November 25, 2014**

Firefox users can type `about:config` into their address bar and then `security.tls.version.min` into the search box. This will bring up the setting that needs to be changed from 0 to 1. The existing setting allows Firefox to use SSLv3 where it's available and if it's required. By changing the setting you will force Firefox to only ever use TLSv1.0 or better, which is not vulnerable to POODLE.



*Chrome

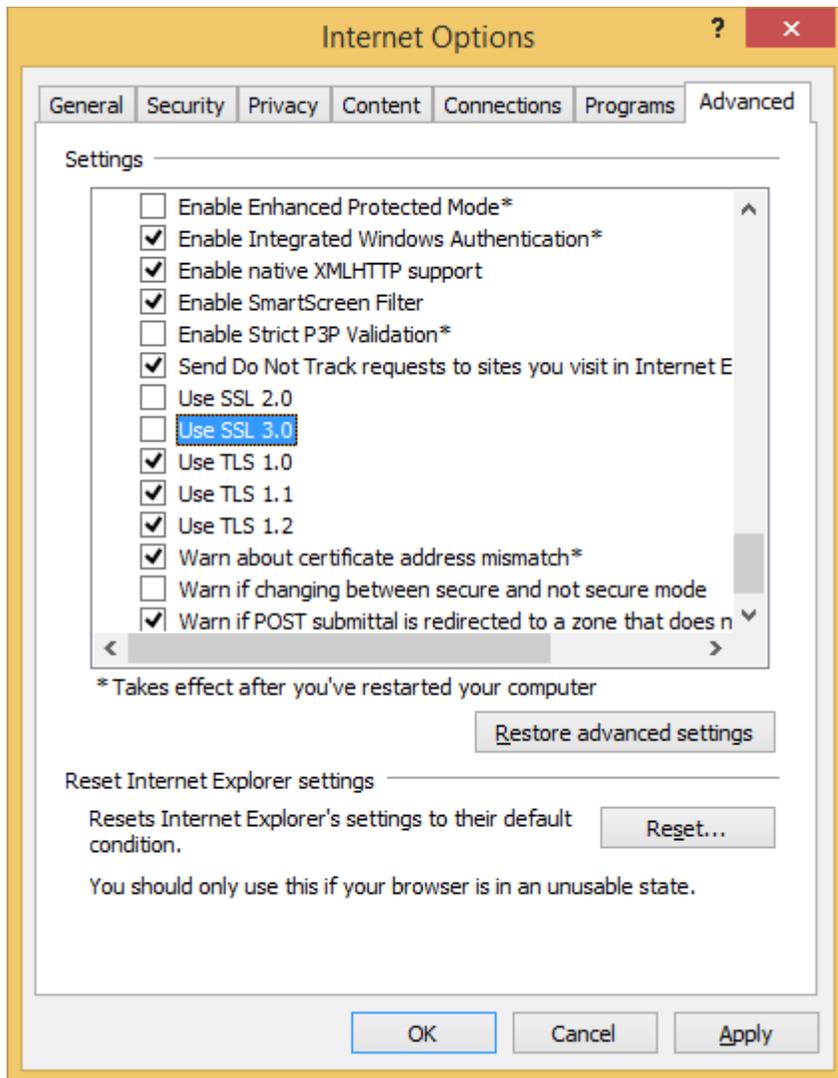
Chrome users don't have an option in the GUI to disable SSLv3 as Google removed it due to confusion over whether SSLv3 or TLSv1 was better with one having a higher numeric value. Instead you can add the command line flag `--ssl-version-min=tlsl1` to enforce the use of TLS and prevent any connection using the SSL protocol. In Windows, right click on your Chrome shortcut, hit Properties and add the command line flag as seen in the image below.



If you use Google Chrome on Mac, Linux, Chrome OS or Android, you can follow these instructions [here](#).

Internet Explorer

Fixing up Internet Explorer is also pretty easy. Go to Settings, Internet Options and click on the Advanced tab. Scroll down until you see the `Use SSL 3.0` checkbox and uncheck it.



HOW TO CHECK YOUR BROWSER

If you want to check that your browser changes have definitely removed SSLv3.0 support there are a couple of sites that you can use. If you visit <https://zmap.io/sslv3/> with SSLv3 enabled in your browser, you will see the warning message I'm getting here in Chrome where I haven't yet disabled SSLv3. To double check the site was working as expected, I disabled SSLv3 support in Internet Explorer and opened up the site there too.

***Firefox and Chrome are not officially supported browsers for Idaho WITS.**