Just In Time for Halloween - - - Zero-day condition - - !

A New Computer Security Exploit - P O O D L E !

Google researchers released news of a vulnerability found in the 15-year old design of SSL 3.0. (SSL = Secure Socket Layer, within the internet data transfer protocol that implements "https.") Since this SSL version has previously been acknowledged as insecure and obsolete, it has already been replaced with the subsequent Transport Layer Security (TLS) model, and TLS is generally in use.

However, the security level offered by SSL 3.0 is still relevant since many web clients implement a protocol downgrade dance. Simply put, this is when web admins are essentially trapped into using this version for it to work with their other legacy systems.

For the Internet public at large, the largest concern is on web browsers and online transactions. Specifically, this flaw may allow attackers to see your online transactions, retrieve payment details, and even change your order—even if you see that trusted secure lock on the upper left corner of your browser!

Fortunately, for using a computer at home, the risk is fairly low, but if you are using a public hotspot, the risk of your "https" connection being hacked is greater. With what researchers have found about SSL 3.0, an attacker can simply conduct man-in-the-middle attacks between the web server and the browser to capture information. Running what they dubbed as the **Padding Oracle On Downgraded Legacy Encryption** or POODLE attack, the group established how this flaw allows an attacker to obtain the plain text of certain parts of an SSL connection, such as the 'secure' HTTP cookie."

Unfortunately, there's no quick patch or easy fix; the flaw is hard-coded *within* SSL 3.0. Browser companies will, in time, be issuing updates to fix this. But, in the meantime:

What to Do: Disable SSL 3.0 in your Internet Browser(s), as described on the following pages. And then you can test if the fix is effective (page 6).

But be aware: After making these adjustments, you might find that business websites don't work properly. So, consider making the following adjustments to one browser but leave a different browser unmodified for those sites that are still waiting for the changes needed to protect themselves from POODLE. (The total fix for this exploit has to happen on both ends of Internet connections – the client and the server.)

Chrome: How to fix the Chrome Browser not to use SSLv3:

Method - in Google's browser, edit the shortcut that launches the browser,
adding a flag to the end of the Shortcut path. Step by step: (written for Windows 7)

1) Start by selecting the icon normally used to launch Chrome.[(a)]

2) Right-click the icon and select Properties. For 32-bit Windows systems do the following: (for 64-bit Windows, see the amended Step 3a below)

3) Under the Shortcut tab, find the box labeled "Target, click in it, and use your keyboard right-arrow key to get to the end of the existing string;
insert a space, then type **--ssl-version-min=tls1** immediately after **chrome.exe"**
It should look something like this (note the space between **.exe"** and **--ssl-**):

"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --ssl-version-min=tls1

(Note: If your original Chrome path doesn't start and end with quotes, don't add one after **chrome.exe.**)

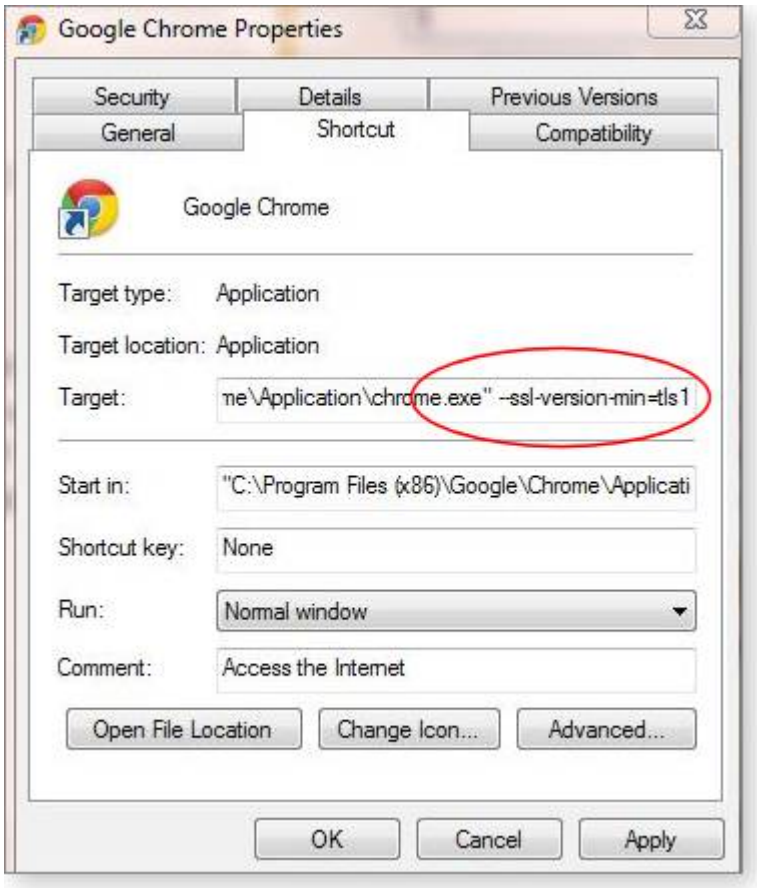


Figure 1. Disable SSL 3.0 support in Chrome by adding a flag at the end of the Properties/Target path.

From now on, launch Chrome only by this edited shortcut. Launching the browser from any unedited launch icons won't provide protection from POODLE. Consider clicking on

the General tab in the Chrome Properties dialog box and giving the edited shortcut a unique name – such as "Chrome - no SSLv3" or something similar. Then you'll always know you're using the right shortcut.

Footnote (a): If your only shortcut to launch Chrome is an icon in your Windows taskbar (at the bottom of the screen) you won't be able to get “Properties” for it. Create a new shortcut, on the Windows Desktop, by
i) Click on “Start”, “All Programs,” and find Google Chrome in the list; right click on it, and click on “Properties” (at the bottom of the menu list.) The Dialog Box that opens should have the Shortcut Tab, and the “Target” fields within it that show in Figure 1.
If no “Target” fields, look to see if the Dialog Box indicates “Type” is a Folder. If so, when you click on “Google Chrome” in the “Start,” “All Programs” sequence, left click on “Google Chrome” to open this folder. Then right-click on “Google Chrome” inside the folder indent. Click on “Properties,” and this time the Shortcut tab and the “Target” fields within that tab should be displayed, matching Figure 1. Now just cancel this Dialog Box.
ii) Repeat “Start,” “All Programs,” as you did just above to find and right click on the “Google Chrome” file, but this time click on “Send to > Desktop (create shortcut).
iii) Go to your Desktop, find the new Chrome shortcut, right-click on it, and select “Properties.” The Dialog box that opens should have a Shortcut tab and Target fields.
iv) For 32-bit Windows systems return to Step 3 in the instructions above Figure 1; for 64-bit Windows, see the amended Step 3a immediately below).

For 64-bit Windows, the text insertion you make needs to be slightly different: *

3a) Under the Shortcut tab, find the box labeled "Target" and insert a space,

then type **/ssl-version-min=tls1** immediately after **chrome.exe"**
It should look something like this (note the space between**.exe"** and /**ssl-**):

"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" /ssl-version-min=tls1

*** reader comment by “rootberg” in Scott Helme's blog on Poodle: https://scotthelme.co.uk/sslv3-goes-to-the-dogs-poodle-kills-off-protocol/**

Firefox: How to fix the Firefox Browser not to use SSLv3:

Firefox 34, due to be released on Nov. 25th, will disable SSL 3.0 support. In the meantime, Mozilla recommends installing an add-on (download site) = https://addons.mozilla.org/en-US/firefox/addon/ssl-version-control/, to obtain "SSL Version Control 0.2" (see Figure 2), which will let you control SSL support within the browser. (Some websites have recommended adjusting Firefox settings in the config. file, but Mozilla recommends using the add-on instead.)

Figure 2. To disable SSL 3.0 support in Firefox, Mozilla offers a browser add-on.

This extension will turn off SSLv3 in your copy of Firefox. When you install the add-on, it will set the minimum TLS version to TLS 1.0 (disabling SSLv3). If you want to change that setting later, such as if you really need to access an SSLv3 site, just go to Tools / Add-ons and click the "Preferences" button next to the add-on. That will give you a drop-down menu to select the minimum TLS version you want to allow.

Internet Explorer:

Click the gear (settings) icon, open **Internet options,** and then select the Advanced tab. Scroll down the Settings list to the Security category, and then look for **Use SSL 3.0.** Uncheck the box (see Figure 3), click OK, and then relaunch IE.

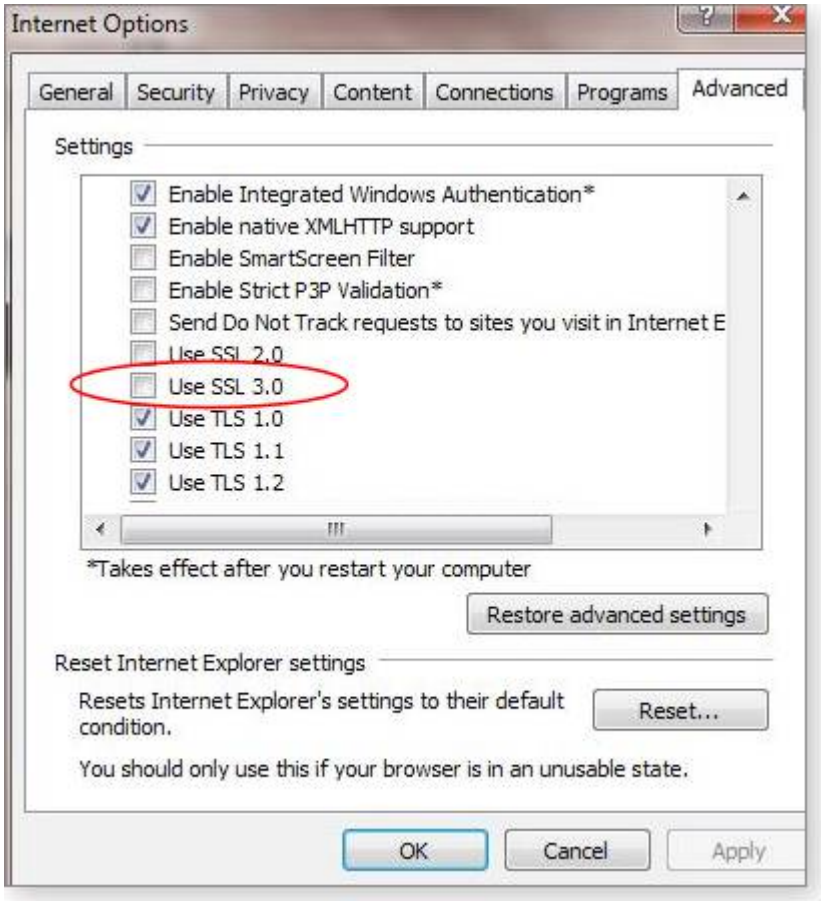


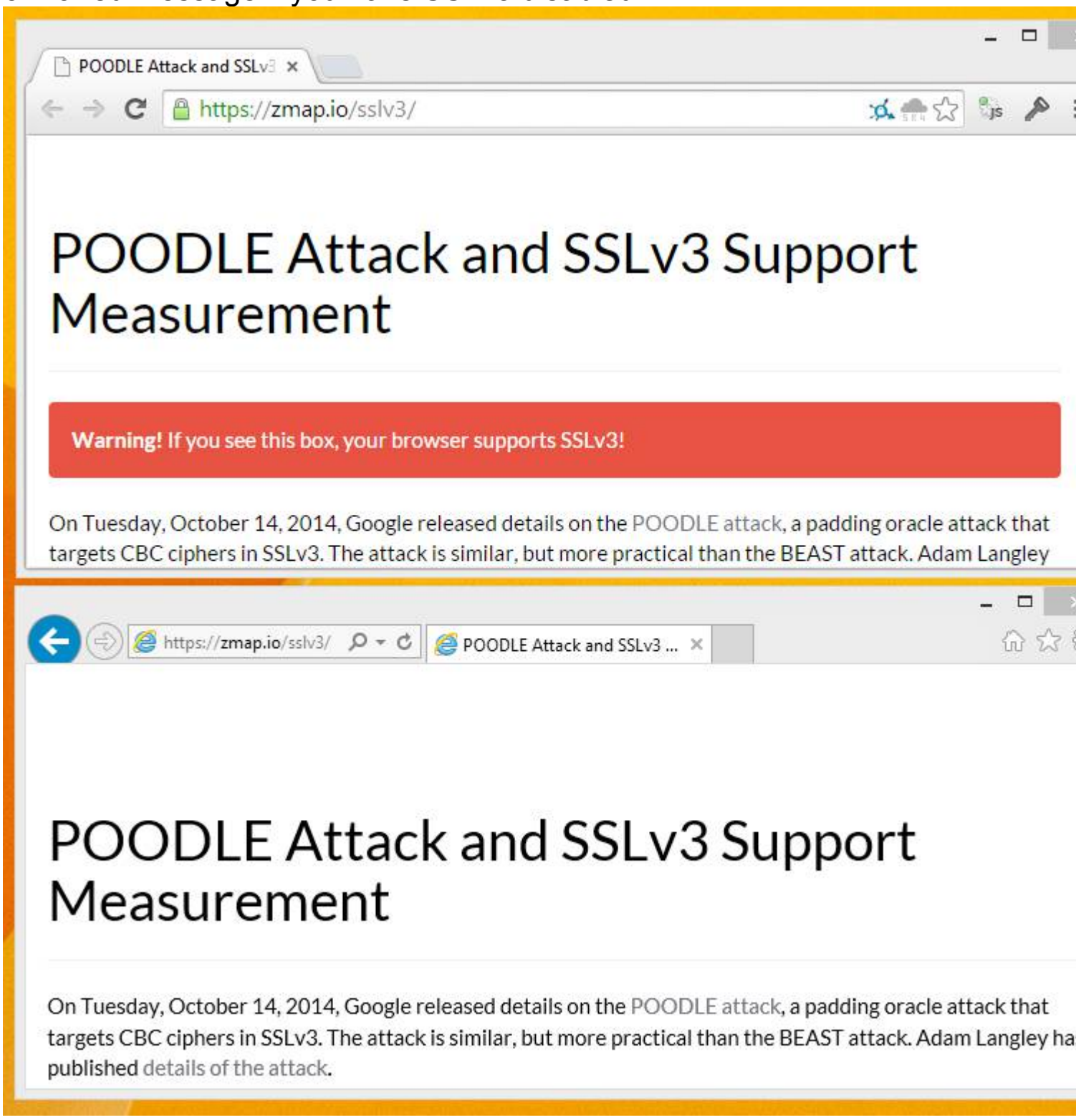
Figure 3. In IE, uncheck "Use SSL 3.0" in the advanced settings dialog box.

Microsoft released an initial security advisory on this topic; expect to see additional guidance in the near future.

(Network admins can make this change to all PCs on the local network via Windows' **Group policy.** Go to the Internet Explorer settings and modify the **Turn off encryption support** object (Windows Components\Internet Explorer\Internet Control Panel\Advanced Page)).

How to test if you're vulnerable to Poodle Exploits: either of two below

https://zmap.io/sslv3/ This test shows the red message if you're at risk, or no red message if you have SSLv3 disabled:



https://www.ssllabs.com/ssltest/viewMyClient.html This Qualys SSL Labs site provides a more detailed analysis of the SSL protocols your browser supports.

[poodletest.com, originally included here, has been removed because it has been found to be an unreliable indicator for Chrome, by several Lex. Comp. Group members. Some Windows Secrets Newsletter blog entries also report getting a false reassurance from poodletest.com] rev. 11/1/14

ed. note: The SSLv3 fixes for Chrome and Internet Explorer were performed in the Lexington Computer & Technology Group meeting October 29th, but I have not "test driven" the Firefox fix.

References: (from which I have cut and pasted material for this paper).

1) Windows Secrets Newsletter, October 23, 2014:
http://windowssecrets.com/top-story/protecting-yourself-from-poodle-attacks/
2) https://scotthelme.co.uk/sslv3-goes-to-the-dogs-poodle-kills-off-protocol/
3) Trend Micro, Inc. (security software house)
http://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/what-to-do-as-experts-reveal-poodle-attack-on-flawed-ssl-3-0

For further reading:

4) Wikipedia, about message transport security:
http://en.wikipedia.org/wiki/Transport_Layer_Security#TLS
5) The OpenSSL organization, presenting Google researchers' paper -
https://www.openssl.org/~bodo/ssl-poodle.pdf
6) How a Padding Attack works:
https://www.imperialviolet.org/2014/10/14/poodle.html

Finally, to point out other Security Fixes (unrelated to Poodle) needed this week, see the article by Brian Krebs below (www.krebsonsecurity.com)

Krebs on Security, October 14, 2014:

Microsoft, Adobe Push Critical Security Fixes

Adobe, Microsoft and Oracle each released updates today to plug critical security holes in their products. Adobe released patches for its Flash Player and Adobe AIR software. A patch from Oracle fixes at least 25 flaws in Java. And Microsoft pushed patches to fix at least two-dozen vulnerabilities in a number of Windows components, including Office, Internet Explorer and .NET. One of the updates addresses a zero-day flaw that reportedly is already being exploited in active cyber espionage attacks.

Earlier today, iSight Partners released research on a threat the company has dubbed "Sandworm" that exploits one of the vulnerabilities being patched today (CVE-2014-4114). iSight said it discovered that Russian hackers have been conducting cyber espionage campaigns using the flaw, which is apparently present in every supported version of Windows. The New York Times carried a story today about the extent of the attacks against this flaw.

In its advisory on the zero-day vulnerability, Microsoft said the bug could allow remote code execution if a user opens a specially crafted malicious Microsoft Office document. According to iSight, the flaw was used in targeted email attacks that targeted NATO, Ukrainian and Western government organizations, and firms in the energy sector.

More than half of the other vulnerabilities fixed in this month's patch batch address flaws in Internet Explorer. Additional details about the individual Microsoft patches released today is available at this link:
(https://technet.microsoft.com/library/security/ms14-oct)

(end)