Surviving Poodle - ColdFusion and SSL 3

Posted At : November 24, 2014 2:45 PM | Posted By : Mark Kruger
Related Categories: ColdFusion, Coldfusion Security, Coldfusion Troubleshooting

There's been a great deal of buzz about *poodle*. Poodle is an SSL exploit capable of highjacking a session using a browser's ability to "negotiate downward" the level of SSL it uses. It's recent prolifieration has put some urgency into the efforts to force existing applications and platforms to deny the use of any standard of SSL less than version 3.0. Super guru Wil Genovese (**Trunkful.com**) recently did some troubleshooting on a ColdFusion server with an issue related to this necessary configuration step. Wil writes:

We ran into an issue when a company contacted us at **CF Webtools** because ColdFusion was suddenly no longer able to connect to their email providers mail servers. One day ColdFusion was sending emails to their clients just fine and the next day it was failing. As you know these issues are usually best resolved by asking "What changed?" As far as the client knew, *nothing* had changed - but we knew enough not to stop digging.

After covering the usual bases on the server we decided to do some very simple testing. For example, does this server connect to *any* mail server? It turns out it was able to connect our mail server without TLS just fine, but it would not connect to that same mail server *with* TLS (TLS is another way of saying SSL 3+). That's the big clue! Checking the Java version I noted they were on JVM 1.7.0_15 which I know is about two years old. Over the last 2 years there have been mandated changes to SSL encryption levels to enforce stronger encryption. This resulted in CA "root" certificates becoming obsolete. To put it another way, if the CA Root Certificates on your system are old they may/will not work with new SSL Certs that use the stronger encryption. In this case we upgraded the JVM version 1.7.0_67 and the problem was resolved. The new JVM versions shipped with the proper root CA certificates. ColdFusion was once again send email through their email providers mail server over a secure (TLS) connection.

The Fix

This issue applies to anyone running anything on Java that needs to access SSL connections. In CFML this includes tags like CFHTTP, CFFTP, CFLDAP, CFMAIL, CFPOP etc. Each of these tags can be used to make a secure connection over SSL. Recently SSL has been undergone some changes and improvements. One of these changes is the *mandatory* increased bit length to 2048 bit that went into effect this year (Muse note: Wil and I are old enough to remember when 40 bit encryption was the industry standard - good times :). If you are curious, this **PDF** file outlines the new requirement.

Since older standards are depricated, all Certificate Authorities have issued new Root CA Certificates along with newly purchased SSL. You may know this if you have installed an SSL certificate recently. You probably had to install the Root CA as well as the SSL Cert.

For Java this means CA Roots that are stored in the Java keystore also need to be updated. You have a couple options depending on the version of ColdFusion you are running and any Java dependancies you may have. If you are running on a fully patched ColdFusion 9, 9.0.1 or 9.0.2 you can run the latest and greatest Java 1.7.0_nn release.

(See my post titled **ColdFusion on Java 1.7** for instructions). Simply upgrading to Java 1.7 will provide you with the lasted CA Root Certificates. The same is true if you are running ColdFusion 10 or 11.

If you are still running on ColdFusion 8 your options are fewer. Of course my standard advice (and Adobe's) is that it's time to upgrade. ColdFusion 8 is no longer supported and it can only run on Java versions that are no longer supported - and which have well documented security flaws fixed in later versions. However, *if you must* run on CF 8, the new CA Root certificates can be installed into your existing Java keystore. The Muse post on **SSL and the trusted keystore** will give you instructions on how to do this. The post is old, but so is your JVM. Again, please consider upgrading to a newer version of ColdFusion! I know it's hard and in some cases expensive - but in the end you will be glad you did.

Here is yet another case for upgrading to Java 1.7 and a newer version of ColdFusion. Several days ago this thread appeared on **CF-Talk**. In summary, to run SOLR on a legacy system you will need to do it at a lower security level. If SSL is restricted to TLS Solr may stop working. Here's some excerpts:

> Michael Grant wrote:
> Fast forward to a few days ago and my host disabled SSLv3, as the world has been instructed to do to thwart the POODLE vulnerability. The moment they did that my app no longer can process transactions. I get the classic "COM.Allaire.ColdFusion.HTTPFailure" type error with the message "Connection Failure: Status code unavailable". This isn't the typical message of when you don't have the cert installed where it says peer could not be authenticated.
>
> According to tech support it's only with CF that disabling SSLv3 stops communication. Apparently others don't have this issue.
>
> Does anyone know of a work around? I'm not sure if CF9 is the problem or CF as a whole. Would upgrading to CF10 help? I'm in a real bind here as the client hasn't been able to process e-commerce transactions for a few days now.
>
> After lots of emails and discussion the solution was to upgrade from Java 1.6 to 1.7... The situation in this case is that the newer Java versions are updated to work with newer SSL standards and have dropped support for the older standards that are now vulnerable to be exploited.

So this is yet another case for upgrading.

Please consider upgrading to a newer version of ColdFusion!

The Muse writes:

Thanks Wil for a great outline of the issues involved with TLS. In case you missed the thrust of his advice, Wil recommends that you upgrade to the latest version of

ColdFusion, and that you *stay up to date* with your JVM versions on existing installations. As always we welcome comments and additions to our online compendium of knowledge. Meanwhile, Wil and I are off to fight the next CF battle.