ColdFusion Security Patches ColdFusion 11 Update 13 and ColdFusion 2016 Update 5

Posted At : September 19, 2017 4:00 PM | Posted By : Wil Genovese
Related Categories: ColdFusion, Coldfusion Security, Coldfusion Upgrading

Adobe just released security updates for ColdFusion 11 and ColdFusion 2016. This is a critical security update and you should be updating your ColdFusion servers. The information below is from the CF Webtools operations group. If you need help upgrading your VM or patching your server (or anything else) our operations group is standing by 24/7 - give us a call at 402-408-3733, or send a note to operations at cfwebtools.com. Meanwhile, this info below will help IT staff and DIY types get started.

With ColdFusion 11 Update 13 and ColdFusion 2016 Update 5 there are additional manual updates that are required to complete the security patch. The additional requirements are the same for both ColdFusion 11 and ColdFusion 2016 and the remaining information pertains to both versions. Both updates require that ColdFusion be running on Java version 1.8.0_121 or higher. For reference, ColdFusion 11 comes with Java version 1.8.0_25 and ColdFusion 2016 comes with Java version 1.8.0_72. The Java that needs to be installed is different from the "Windows User" Java client that may already be installed. The installer is available from Oracle. Once the new Java version installed, the jvm.config file for each ColdFusion instance needs to be updated to point to the new Java version installation path. If you're running the Enterprise version of ColdFusion, there's a likely chance there is more than one ColdFusion instance running.

Part of the instructions from Adobe says that if your ColdFusion server is installed as J2EE server then there is an addiction manual configuration that you ned to do. However, every installation of ColdFusion since the release of ColdFusion 10 is a J2EE or JEE installation. What Adobe really meant was that if you are using a third party JEE server and not the built-in Tomcat JEE server.
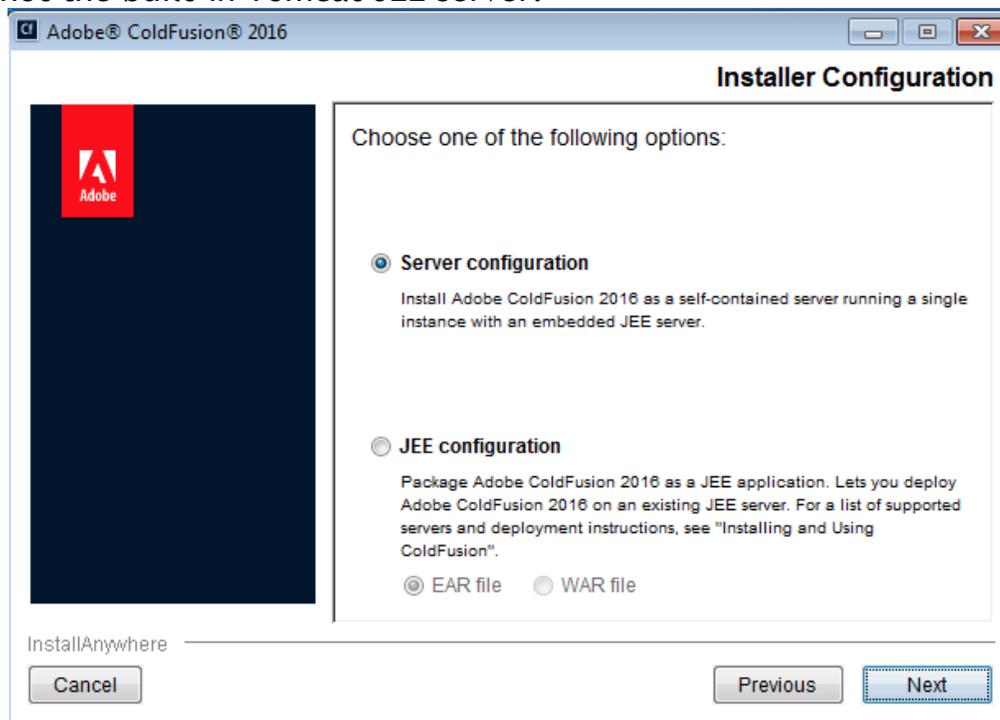
If your ColdFusion server is running on a third party JEE server such as WebLogic, Wildly, custom Apache Tomcat, etc (Not the built in Tomcat that comes with ColdFusion), then the following step needs to be completed.

Set the following JVM flag, "-Djdk.serialFilter=!org.mozilla.** ", in the respective startup file depending on the type of Application Server being used.

For example,

- On Apache Tomcat Application Server, edit JAVA_OPTS in the 'Catalina.bat/sh' file
- On WebLogic Application Server, edit JAVA_OPTIONS in the 'startWeblogic.cmd' file
- On a WildFly/EAP Application Server, edit JAVA_OPTS in the 'standalone.conf' file

This is one more friendly reminder to make sure your ColdFusion servers are patched! Either patch them yourself, have your hosting provider patch them or if they are not familiar or knowledgeable with ColdFusion contact us at **CF Webtools** to patch your servers.

As always, if you need help migrating to the next version, scanning your ColdFusion server for security vectors or installing this patch and new Java version, contact your project or account manager directly, or send an email to support@cfwebtools.com. You can also simply respond to this email (or call 403-408-3733).

Note: ColdFusion11 when it was first released came with a version of Java 1.7.0_nn. Adobe later re-released ColdFusion 11 with Java 1.8.0_25. If you have ColdFusion 11 still running on Java 1.7 I highly recommend that Java be upgraded to Java 1.8. Oracle is no longer supporting Java 1.7 and 1.7 is long past it's end of life. Even though the Adobe instructions for this current security update states that you can run Java 1.7.0_131, I highly recommend upgrading to Java 1.8.