ColdFusion Security updates for ColdFusion 2016 and ColdFusion 11

Posted At : April 10, 2018 2:03 PM | Posted By : Wil Genovese
Related Categories: ColdFusion, Coldfusion Security

Adobe released important security updates and big fixes today, update 6 and update 14 for ColdFusion 2016 and ColdFusion 11 respectively.

> These updates resolve an important insecure library loading vulnerability (CVE-2018-4938), an important cross-site scripting vulnerability that could lead to code injection (CVE-2018-4940) and an important cross-site scripting vulnerability that could lead to information disclosure (CVE-2018-4941). These updates also include a mitigation for a critical unsafe Java deserialization vulnerability (CVE-2018-4939) and a mitigation for a critical unsafe XML parsing vulnerability (CVE-2018-4942).

There is a bug of great importance to many that has finally been fixed. I've blogged about this before and I was able to create a work around to resolve this issue until it was fixed by Adobe. The SFTP/FTPS bug would not allow connections to secure FTP servers that utilized newer SSL protocols. When using CFFTP to connect to some S-FTP server, during connection, you can see an error message. This has been a growing issue as more and more companies replace plain text FTP servers with SFTP or FTPS servers that utilize stronger protocols.

For ColdFusion 2016 this update upgrades Tomcat to version 8.5.28 and OpenSSL to version 1.0.2n.

For ColdFusion 11 this update upgrades Tomcat to version 7.0.85 and OpenSSL to version 1.0.2n.

The security updates referenced in the above Tech Notes require JDK 8u121 or higher (for ColdFusion 2016) and JDK 7u131 or JDK 8u121 (for ColdFusion 11).

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. 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.

**Note: ColdFusion 11 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. Personally I will not install Java 1.7 on a clients servers and sign off on it being 'secure'.*