Certain JPGs Can Crash Your ColdFusion 8 Server

Posted At : June 10, 2009 11:41 AM | Posted By : Mark Kruger
Related Categories: ColdFusion, Coldfusion Troubleshooting

This issue was brought to my attention by Adrian Lynch on CF-Talk. It seems that if you use the new image functions in ColdFusion 8 against certain kinds of JPG images you can actually cause your JVM to crash. If you have code that uses the latest image functions to handle uploaded images you should definitely take note of this post. I cannot yet see how a user might take advantage of this bug to penetrate your server, but a malicious (or even non-malicious) user could easily perform a denial of service attack and cause your CF server to go up and down like Jack LaLanne doing jumping jacks. So if you fit into that category (handling uploaded images using CF 8 image functionality) here's the scoop.

JPG "ICC" Profile

A JPG image has something (optionally) embedded in it called an "image color correction" profile. It is actually a bit of meta data that tells a browser or other image rendering program how to show the image on the screen. To see the profile, take an ordinary JPG and run this code:

```
<Cfset info = ImageRead(ExpandPath("./sample.jpg"))/>

<cfdump var="#info#"/>
```

What you should see is the standard "dump" output showing whatever information can be gleaned from the image file itself about what it is and how to display it. Something like this:

struct		
colormodel	struct	
	alpha_channel_support	NO
	alpha_premultiplied	NO
	bits_component_1	8
	bits_component_2	8
	bits_component_3	8
	colormodel_type	ComponentColorModel
	colorspace	Any of the family of RGB color spaces
	num_color_components	3
	num_components	3
	pixel_size	24
	transparency	OPAQUE
height	1780	
source	C:\ColdFusion8\wwwroot\sample.jpg	
width	1280	

Notice the "clolor model" structure and keys. I could be wrong but I take that to be the ICC profile. Now it just so happens that there is a bug in the parser for this ICC Profile. Not the ColdFusion parser, but the underlying parser used by the javax.imageio classes - the ones used by CF under the hood to make this "imageRead()" magic happen. Under certain conditions information in the ICC Profile will be parsed incorrectly and cause a

buffer overflow. This in turn abends the entire JVM and causes your ColdFusion server to restart.

Sample JPGs

If you would like to test this and see for yourself, here are 3 images that will do the trick for you.

- http://www.coldfusionmuse.com/images/icc_sample1.jpg
- http://www.coldfusionmuse.com/images/icc_sample2.jpg
- http://www.coldfusionmuse.com/images/icc_sample3.jpg

All you have to do is try running the code above on one of these images using JVM version 1.6.0_04 and you will see your server restart. This article on the **JDK IMage Parsing Library Vulnerabilities** is where I found enough information to draw my conclusions and make my tests.

The Fix

Fortunately the fix is pretty easy. Upgrade your JVM to 1.6.0_05 or above (current distribution is 1.6.0_14). In the newer build of the 1.6 engine this vulnerability is fixed. Now, if you are using CF 8 with JVM 1.5 (as some folks are) I would be interested to know if this issue is relevant. I could be that it only affects 1.6.0 to 1.6.0_04. Perhaps one of my readers would test it find out. Meanwhile, if you accept images uploaded to your server and you are taking advantage of any of the ColdFusion 8 image libraries (like imageRead() above), then you should probably upgrade ASAP. It's only a matter of time before someone uploads an image that crashes your server.