ColdFusion Server Infection Using the Missing Template Handler

Posted At : December 5, 2013 1:29 PM | Posted By : Mark Kruger
Related Categories: Coldfusion Security

We were recently called to fix a hacked ColdFusion server. This was a file hack. Something was appending JS code to the end of variuos .cfm files on the server. The appended code redirected the user's browser to a different site (to sell them viagra or puppies or whatever). When analysing the server we found an interesting attack vector. I say interesting because it used a technique I had not seen before that leveraged a quirky feature of ColdFusion. The end result of the hack was a layered infection that was difficult to find and resulted in the infected files coming back regardless of our lockdown efforts. If that sounds like something you are experiencing or if you are interested in ColdFusion security, read on!

To understand it you need to understand the nuances of the "missing template handler." This is a page you specify in the CF Admin. The setting looks like this:

To use this setting you need to remember it is a "global" error handler. So ColdFusion needs to be able to *find and execute* this template from any site on the server with ColdFusion enabled. What may be less clear is that ColdFusion is going to execute this file in the same fashion as a cfinclude. It is going to open, parse, compile and execute any CF code it finds in it. Some clever Muse readers utilize the trick of "including" a file with a different extension other than ".cfm." This can be an appropriate security measure if you want to insure that a file cannot be executed via the URL. The most common include extension that is *not* .cfm is .inc, as in:

```
<cfinclude template="blah.inc"/>
```

So with an include it doesn't matter what the file is called. It could be called "blah.txt","blah.log" or even "blah.doc." No matter what is specified ColdFusion will attempt to open and parse the file as a CF source file. If it finds ColdFusion code it will compile and execute it. That's the way ColdFusion treats the "missing template handler" as well. You can put the handler anywhere you like, even somewhere not accessible via a URL, call it whatever you want, and CF can still run the file.

Meanwhile back to our attack. We found that a specific file (ttextt.cfm) was wreaking havoc by appending malicious JavaScript code to the end of all the cfm files it found. We locked down all the vectors that are open to file based attacks, deleted the file and removed all offending code from the cfm pages of course. But after lock down, deleting the file did not work. It was back in place within a few minutes. That had us looking deeper batch files, vbs scripts and (of course) ColdFusion code able to create the ttextt.cfm file. We found such code in the root mapping in a file named "license.log." This file contained ColdFusion code able to regenerate ttextt.cfm - but that made us even more curious. Opening "/license.log" using a browser and the domain would not work. IIS did not have a handler for .log files to serve them as web

pages. Moreover even if IIS was set up to server .log files the most likely result would be serving it as text, not running it as CFML - so you would simply see the CF code in your browser. It was head scratching.

Finally, perusing the admin settings, we noticed that "license.log" was entered as the default missing template handler. The result? All the hacker had to do was *attempt to load any non-existent ColdFusion template*. That's right, the hacker could simply reinfect the server by hitting /blah/1234.cfm. If 1234.cfm did not exist ColdFusion would call the "missing template handler" (license.log) as an include and execute whatever CFML it found there - in this case the code to recreate the ttextt.cfm.

Why go through all this trouble? It does seem like a good bit of trouble. If you are already able to do things like change the missing template handler and upload license.log to the server, do you really need an additional back door? I suppose the main result is a vulnerable server that is hard to disinfect. Shutting down FTP and Webdav, Patching ColdFusion, patching CKEditor, analyzing and fixing cffile code etc. - all of these might plug the original hole but *none* of these fixes would keep ttextt.cfm from coming back. Disabling file creation would do it but that's not an option for most ColdFusion servers which use such features regularly. Then too, the file "license.log" looks both important (ooh, it's a license file, if I delete it bad things could happen!) and innocuous (it's just a log file after all). Finally, that missing template handler is not a setting you check every day - or believe to be broken - unless you use it to do something very specific (besides just catching bad cfm requests). So it's an ingenious layered attack with entrenched lines that you have to dig through to fix.

The takeaway? If you have a file based hack on your server, be sure and check the missing template handler setting. Good luck out and may the Muse be with you.

Muse Note: I had nothing to do with this fix or the information I'm presenting here. This hack was found and fixed by Super Guru Wil Genovese (**trunkful.com**) who is my great friend and with whom I have the privilege to collaborate.