Vulnerability in Allaire ColdFusion v.4 and earlier

Jeff Dahlberg
September 11, 2000

ColdFusion from Allaire

ColdFusion is a Web Application Server Package from Allaire Corporation that can be used to develop and deliver e-business applications. ColdFusion developers use the ColdFusion Markup Language to cleanly integrate ColdFusion functionality into HTML pages.

As a service to new developers, Allaire created sample applications that they included with the documentation. By viewing and using these sample applications, developers get to see ColdFusion in action and quickly get an understanding of ColdFusion's capabilities and methodologies.

The Vulnerability

The Allaire ColdFusion default installation includes the ColdFusion Documentation and sample applications. One of these applications is supposed to allow only users on the localhost to upload, execute, display and delete expressions that they are testing. By misusing one of the sample applications, a web-browsing user can remotely delete, display, upload and execute any ColdFusion file in the system.

The expression evaluator sample application gives users the ability to execute ColdFusion expressions as they experiment during development or learning. The web-browsing user can upload a file, which is than processed, displayed and deleted. This application is usually restricted to the localhost machine but the web-browsing user can access pages in this application and by sending a crafted URL can display and delete the file of their choice on the server.

The sample application "Expression Evaluator" is comprised of many files including Openfile.cfm, openedfile.cfm and ExprCalc.cfm. The web-browsing user can upload a file using "Openfile.cfm" and "openedfile.cfm". Then the file is displayed and deleted using "Exprcalc.cfm". The vulnerability that can be exploited with this application is that "Exprcalc.cfm" can be used to delete itself. Than the web browsing user can use "Openfile.cfm" and "openedfile.cfm" to upload and execute a file that will not be deleted.

Illustration

'A' is used for the Attacker
'V' is used for the Victim

1. 'A' scans your network looking for cold fusion server.
2. 'A' locates a cold fusion server 'V' on your network.
3. 'A' sends "http://www.V.com/cfdocs/expeval/openfile.cfm.

4. ‘V’ responds to ‘A’ with “http://www.V.com/cfdocs/expeval/ExprCalc.cfm?

   RequestTimeout=2000&OpenFilePath=C:\Inetpub\wwwroot\cfdocs\expeval\.\dummy.txt”
5. ‘A’ changes the URL from “…dummy.txt” to “…ExprCalc.cfm” to delete the program that is about to delete dummy.txt. This causes ExprCalc.cfm to delete itself, which allows ‘A’ to upload files using openfile.cfm without the delete step from ExprCalc.cfm.

Possible Uses of the Vulnerability

One of the major uses of this vulnerability is web site defacing. By following the above steps, the attacker can replace the main page, which is often index.html. A much more devious attack would include modification of the main page to cause sideline information transmission to the attacker. This could include collection of personal information or financial information including credit card numbers.

Are you vulnerable?

You are vulnerable if you are running Allaire’s ColdFusion Server 4.0 or earlier with the documentation and examples installed. This problem was resolved in the 4.1 release but Allaire does not recommend running production servers with the documentation and examples installed.

How do you fix it?

Allaire has recommendations to fix this vulnerability. The first option is to remove the documentation directory called CFDOCS. This is the best fix you could implement because this vulnerability and any future vulnerability that may arise from CFDOCS applications would be resolved. It is recommended generally that you keep sample code and documentation on secured developer workstations and ensure that you do not have sample code and documentation on any production servers.

For those who need to have the sample code and documentation in the production environment, Allaire offers a patched version of the Expression Evaluator. This patch can be downloaded from the Allaire web site and enforces the local user requirement on using the expression evaluator sample application.

Conclusion

In the Allaire ColdFusion Web Application Server package, versions 4.0 and earlier, a vulnerability exists that allows non-local web users to upload, execute, view and delete files on the webserver. This vulnerability can be easily countered by uninstalling the ColdFusion documentation and sample applications from all production web servers. If it is necessary for you to have the documentation and sample applications on a production server, download and apply the Expression Evaluator patch that Allaire has made available on their website.

Sources

"Allaire: ColdFusion: ColdFusion Product Information."
URL:http://www.allaire.com/Products/ColdFusion/productinformation/, (9/11/2000)

"Allaire ColdFusion Remote File Display, Deletion, Upload and Execution Vulnerability." Bugtraq ID 115, published December 25 1998, URL: http://www.securityfocus.com/, Vendor=Allaire Title=ColdFusion Server, (9/11/2000)

"Another Cold Fusion Server vulnerability 9/7/99."
URL:http://www.securiteam.com/exploits/Another_Cold_Fusion_Server_vulnerability.html, (9/11/2000)

"Expression Evaluator Security Issues." Allaire Security Bulletin (ASB99-01)Expression Evaluator Security Issues Originally Posted: February 4, 1999
Last Updated: April 30, 1999,
URL:http://www.allaire.com/handlers/index.cfm?ID=8727&Method=Full, (9/11/2000)