Global Information Assurance Certification Paper

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)

Last Updated: September 19th, 2017

Upcoming Training

Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401*	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Oct 03, 2017 - Nov 14, 2017	Mentor
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401*	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401**	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS