Locking Down ColdFusion Pete Freitag, Foundeo Inc.



Wednesday, August 4, 2010

Who am I?

- Over 10 years working with ColdFusion
- Owner of Foundeo Inc a ColdFusion consulting & Products company
- Author, Blogger, and Twitterer?

Today's Agenda

- Security Concepts Applied
- Secure Installation Tips
 - Windows 2008 / IIS 7
 - RedHat EL 5.3 / Apache 2.2
- Secure Configuration Tips

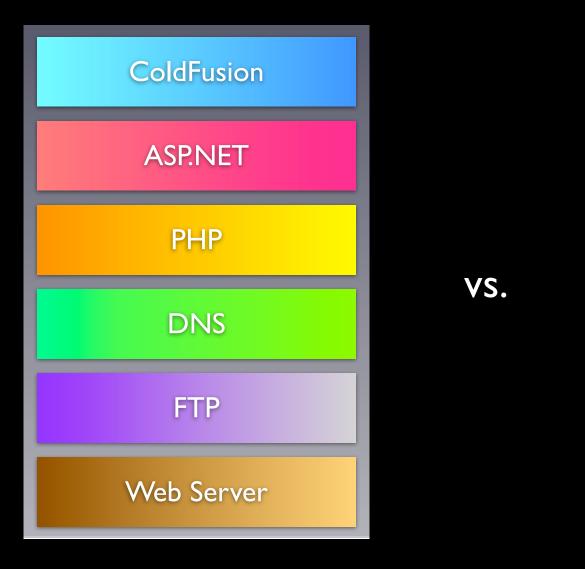
Disclaimer

- It's simply not possible to cover everything there is to know and do to setup a secure ColdFusion server in this I hour session.
 - I'll point you to resources as we go

CF9 Lockdown Guide

- This presentation is based on the ColdFusion 9 Lockdown Guide I wrote for Adobe:
 - <u>http://www.adobe.com/products/</u> <u>coldfusion/whitepapers/pdf/</u> <u>91025512_cf9_lockdownguide_wp_ue.pdf</u>
 - <u>http://bit.ly/cf9secure</u>

Reduce Attack Surface



ColdFusion Web Server

Wednesday, August 4, 2010

Defense in Depth

- A layered approach to security.
- Reduces the risk of vulnerabilities in one of the levels.

Network Firewall

Web App Firewall

Web Server Rules

Application Server Rule

Your Source Code

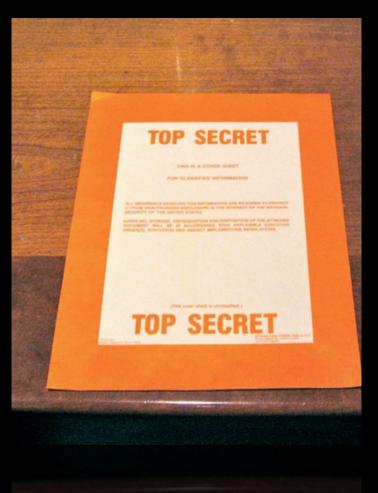
Database Controls

Defense in Depth Example

- Web App has read only access to a database.
 - Setup datasource to only allow SELECT
 - Setup sandbox to only allow access to the given datasource
 - Setup database user privileges to only allow SELECT.

Principle of Least Privilege

 Grant the minimum amount of permission necessary to do the job.



Defaults

 Changing defaults doesn't necessarily make you more secure, but it does make automated attacks less likely to succeed.

Logging

- Important for monitoring & forensics.
- Regulations & Requirements
 - Example: PCI requires you to retain logs for at least one year.

Before You Install

• Create 3 Partitions:

- OS
- ColdFusion
- Web Assets

Wednesday, August 4, 2010

Install OS

- Install with minimal components
- Refer to security guides for installing and configuring OS:
 - NSA Security Configuration Guides:
 - <u>http://www.nsa.gov/ia/guidance/security_configuration_guides/</u>
 - Microsoft Security Compliance Manager
 - <u>http://www.microsoft.com/downloads/details.aspx?</u> FamilyID=5534bee1-3cad-4bf0-b92b-a8e545573a3e&displaylang=en

SELinux

- ColdFusion can run under Security Enhanced Linux with a little effort.
- Install with SELinux Enforcing mode on
- SELinux allows programs (such as apache) to run in their own sandboxed security domains.

User Accounts

- ColdFusion runs under the System account on Windows.
- Create user accounts for ColdFusion and the web server to operate under.

User Accounts

- Remove unnecessary permissions and default groups.
- On Windows
 - Deny Terminal Services Access
- On Linux
 - Shell: /sbin/nologin *
 - Add to /etc/nologin

* Requires modifying the cf startup script

ColdFusion User

Directory	Read	Write
ColdFusion Root	Y	Yes many sub directories require write (logs, etc)
Web Root	Y	As needed

Run ColdFusion As

Services
 Right Click
 Log On tab
 Enter Credentials

	covery Dependencies	
Log on as:		
C Local System acco	u nt interact with desktop	
This account:	cfusion	Browse
Password:	•••••	
Confirm password:	•••••	
	<u>r account log on options.</u> able this service for the hardv	vare profiles listed bel
	<u>r account log on options.</u> able this service for the hardw	vare profiles listed belo
You can enable or disa		
You can enable or disa Hardware Profile	ble this service for the hardv	Enabled

Run ColdFusion As...

• On Linux

 The ColdFusion installer will prompt you for a user name to run ColdFusion as.

Web Server User Permissions

 The web server user will need file system permissions to the lib/wsconfig directory under your ColdFusion installation.

Apache User

- Found in the Apache conf file: httpd.conf
 - User apache
 - Group apache
 - Some installations will use the account: nobody but it's better to use a dedicated account.

IIS App Pool User

- Microsoft does not recommend changing the run as account for the World Wide Web Publishing Service.
 - Instead you can modify the *Identity* (the user) that each IIS Application Pool Runs As.
 - Application Pools > Actions > Set Application Pool Defaults > Process Model > Identity

File Auditing

- Modern Operating Systems allow you to log successful or failed file access attempts.
 - Be careful logging all successful file operations, can quickly fill logs.
 - Successful deletes are a good idea though.
 - Log all failed accesses (read, write, delete, etc).

Linux File Auditing

• Use **auditd** for Linux (Linux Kernel 2.6+)

- Config stored in: /etc/audit.rules
- auditctl modify rules
- ausearch search logs
- aureport reports logs

Windows Advanced Security

Right Click on a Directory
 Select the Security Tab
 Click Advanced

web Properties	×
General Sharing Security Previous Versions Customize	
Object name: F:\web	
Group or user names:	
& CREATOR OWNER	
SYSTEM	
Administrators (IP-0AF327C3\Administrators)	
Sers (IP-0AF327C3\Users)	
To change permissions, click Edit. Edit	
Permissions for CREATOR OWNER Allow Deny	
Full control	
Modify	
Read & execute	
List folder contents	
Read	
Write	
For special permissions or advanced settings, Advanced	
Learn about access control and permissions	
OK Cancel Apply	

Windows File Permissions

Туре	Name	Permission	Inherited From	Apply To
Allow	Administrators (IP-0AF327	Special	<not inherited=""></not>	This folder only
Allow	Administrators (IP-0AF327	Full control	F:\	This folder, subfolders and
Allow	SYSTEM	Full control	F:\	This folder, subfolders and
Allow	CREATOR OWNER	Special	F:\	Subfolders and files only
Allow	Users (IP-0AF327C3\Users)	Read & execute	F:\	This folder, subfolders and
Allow	Users (IP-0AF327C3\Users)	Special	F:\	This folder and subfolders
	e inheritable permissions from this	s object's parent		

Windows Auditing

missions	Auditing Owner Effe	ective Permissions			
bject nam	e: F:\web	g entry, select the entry and	then click Edit.		
uditing ent Type	tries:	Access	Inherited From	Apply To	
Edit.	N				
		es from this object's parent			
7 Include					

Windows File Auditing

Auditing Entry for web Object			×
Name: Everyone		Change.	
Apply onto: This folder, subfolders	and files		•
Access:	Successful	Failed	
Full control Traverse folder / execute file List folder / read data Read attributes Read extended attributes Create files / write data Create folders / append data Write attributes Write attributes Write extended attributes Delete subfolders and files Delete			
Managing auditing Managing auditing		Clear A	

Create a ColdFusion Administrator Site

- The ColdFusion Administrator Should not be exposed to the public.
- Setup a dedicated web site on the web server.
- Listen on localhost only or a internal lan address
- Require SSL.
- Use a Web Server Password to allow Auditing.

Install ColdFusion



Don't Install Everything

Adobe ColdFusion 9	Subcomponent Installation
 Introduction License Agreement Configure Installer Configure ColdFusion Pre-Installation Summary Installing Installation Complete 	Select the subcomponents to install: ColdFusion subcomponents ColdFusion 9 ODBC Services ColdFusion 9 Search Services ColdFusion 9 Solr Services NET Integration Services ColdFusion 9 Documentation
nstallAnywhere	Previous Next

No RDS on Production

Adobe ColdFusion 9

_ 🗆 🗙

Enable RDS

 Introduction License Agreement Configure Installer Configure ColdFusion 	The ColdFusion Remote Development Service (RDS) lets developers using Adobe tools remotely connect to this server for development purposes. RDS is required for Line Debugging, Report Builder, and Dreamweaver Extensions.
 Pre-Installation Summary Installing Installation Complete 	If this is a production server, Adobe recommends that you disable RDS. Note, however, that disabling RDS also disables debugging, the directory browsing applets in the ColdFusion Administrator and some of the functionality in the Report Builder.
	Enter password:
nstallAnywhere	Confirm password:
Cancel	Previous

ColdFusion Administrator

ColdFusion Administrator Lo X C A C A Marco Los X C A C A Marco Los X C A Marco Los X C A C A Marco Los X
ADOBE" COLDFUSION" 9 ADMINISTRATOR User name admin Password Login Adobe, the Adobe logo, ColdFusion, and Adobe ColdFusion are trademarks or registered trademarks of
Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

Wednesday, August 4, 2010

Sandbox Security

• Restricts what your CFML can access:

• Tags

- Functions
- Datasources
- File Access
- Network

Sandbox Setup

- Very easy to get going with on standalone install (click checkbox).
- Enterprise / Mutilserver requires an addition to jvm.config
- Enterprise allows multiple sandboxes

Sandbox jvm.config

-Djava.security.manager "-Djava.security.policy=cf_root/WEB-INF/cfusion/ lib/coldfusion.policy" "-Djava.security.auth.policy=cf_root/WEB-INF/ cfusion/lib/neo_jaas.policy"

Restricting /CFIDE

- Expose only the necessary files in /CFIDE
- Many of the files can be blocked by the web server but still work within ColdFusion.

What's in /CFIDE

Folder / File	Notes
adminapi/	ColdFusion Admin API, can usually be blocked.
administrator/	CF Admin, should not be public.
AIR/	Adobe Air offline synchronization. BINU
appdeployment/	Used for CAR File Deployment, can be blocked.
classes/	Contains Old CFForm Applets. BINU
componentutils/	CFC Metadata Documentation, should not be public.
debug/	Used when debugging is enabled, should not be public.

BINU = Block if not used

What's in /CFIDE

Folder / File	Notes
images/	Contains 2 image files, should be safe to block.
orm/	ORM Event Handler Interface CFCs. Can be blocked.
portlets/	CF9 Portlet API. BINU
probe.cfm	ColdFusion Probes. BINU
scripts/	JS, CSS, and CFM files used by cf tags. Move to non- default location, or BINU.
ServerManager/	Contains Server Manager AIR app. Can be blocked.
services/	CFAAS Components. BINU
wizards/	Not sure what its for but it has had several vulnerabilities in the past year or so. Block it.

BINU = Block if not used

Blocking /CFIDE

- Apache mod_rewrite
- IIS 7 applicationHost.config file

<denyUrlSequences>
 <add sequence="/CFIDE/administrator" />
 <add sequence="/CFIDE/adminapi"/>
 <add sequence="/CFIDE/AIR"/>
 <add sequence="/CFIDE/appdeployment"/>
 <add sequence="/CFIDE/componentutils"/>
 <add sequence="/CFIDE/debug"/>
 <add sequence="/CFIDE/orm"/>
 <add sequence="/CFIDE/orm"/>
 <add sequence="/CFIDE/portlets"/>
 <add sequence="/CFIDE/probe.cfm"/>
 <add sequence="/CFIDE/services"/>
 <add sequence="/CFIDE/services"/>
 <add sequence="/CFIDE/services"/>
 <add sequence="/CFIDE/services"/>
 <add sequence="/CFIDE/services"/>
 <add sequence="/CFIDE/wizards"/>
 <add sequence="/CFIDE/services"/>
 <add sequence="/CFIDE/services"/>
 <add sequence="/CFIDE/services"/>
 <add sequence="/CFIDE/wizards"/>
 <add sequence=>
</add>

IIS 7 Request Filtering

• Take some time to learn about it.

- Block by URI
- Block file extension white/black list
- Limit POST Size, Query String size
- Limit Verbs (GET, POST, etc)

What's not in /CFIDE

- You might notice that a few other requests are served from /CFIDE but don't have corresponding files. For example:
 - /CFIDE/GraphData.cfm (cfchart)
 - /CFIDE/main/ide.cfm (RDS)

Servlet Mappings

• These mappings are defined in the <u>web.xml</u> file located in the WEB-INF directory.

• <u>web.xml</u> is part of JEE / J2EE standard

Servlets & Mappings

- Java EE Web Applications consist of Servlets and Servlet Mappings.
 - Servlet Is the chunk of code that does the processing of the request
 - Servlet Mapping Simply routes url requests to a Servlet.

Example Servlet Mapping in <u>web.xml</u>

<servlet-mapping id="coldfusion_mapping_11">
 <servlet-name>GraphServlet</servlet-name>
 <url-pattern>/CFIDE/GraphData.cfm</url-pattern>
 </servlet-mapping>

Removing Unused Mappings

- You can remove unused servlet mappings by commenting out the <servlet-mapping> tags in <u>web.xml</u>
 - Warning: Keep a backup of the <u>web.xml</u> file certain changes might cause the server not to start. Strict XML.
 - Beware Adobe may not preserve your changes when installing an updater.

Servlet Mappings in CF9

URI Mapping	Servlet	Used For
*.cfm, *.cfml	CfmServlet	Serving cfm files. Don't remove
*.cfc	CFCServlet	Serving Remote CFC Method calls.You can remove this mapping and still use CFCs, you just can't use remote methods.
/CFIDE/GraphData.cfm /CFIDE/GraphData	GraphServlet	CFChart, CFGraph
/flashservices/gateway/*	FlashGateway	BlaseDS for Flash Remoting
/flex2gateway/*	MessageBrokerSer vlet	Flash Remoting for Flex
*.jws	CFCServlet	Web Services written in java, not typically used by CF developers.

Servlet Mappings in CF9

URI Mapping	Servlet	Used For
*.cfr	CFCServlet	CFReport
/CFFormGateway/*	CFFormGateway	CFForm Flash Forms
/cfform-internal/*	CFInternalServlet	CFForm Flash Forms
*.cfswf	CFSwfServlet	CFForm Flash Forms
/CFFileServlet/*	CFFileServlet	Used for serving images from cfimage tag. Also used in cfreport and cfpresentation
/WSRPProducer/*	WSRPProducer	Web Services for Remote Portlets

HackMyCF.com

- Free ColdFusion Security Scan
 - Enter your email & domain to get a free report
- Paid Subscription:
 - Automated Scans
 - Additional Features
- <u>http://hackmycf.com/</u>

000	hackmycf: test.foundeo.com — Starred	0		
	col Scol Col (C) (V) rphy Reply All Forward Print To Do			
From: Foundeo «peter		E.		
Subject: hackmyst:test.foundee.com Dute: October 20, 2009 12:56:39 PM EDT				
To: peteril/foundeo.o				
hackmycf				
We found 9 security issues on your server test.foundeo.com				
CRITICAL	Robust Exception Information is Enabled Robust Exception Information is enabled which leads to path disclosure and partial source code disclosure			
CRITICAL	File Uplead Vulnerability in CF8 FCKeditor The C5 uplead C4m and C5 connector cfm files must be deleted. This allows a remote user to uplead a CFM file to the server. Nore information: <u>http://www.adobe.com/support/securits/bulletins/apub0H-0E.html</u>			
CRITICAL	Cross Site Scripting Vulnerability CVE-2009-1877 CVE-2009-1877 detected. Apply the hotfoxes located in Adobe Security Notice apsb09-12 Nore Information: <u>http://www.adobe.com/support/securits/bolletins/apsb09-12.html</u>			
CRITICAL	Cross Site Scripting Vulnerability CVE-2009-1872 CVE-2009 1872 detected. Apply the hotfixes located in Adobe Security Notice apsb09-12 Wore Information: <u>http://www.adobe.com/support/security/bolletins/apsb09-12.html</u>			
IMPORTANT	ColdFusion Administrator is Public ColdFusion Administrator should be restricted by IP or blocked with Web Server password protection. Also consider requiring a SSL connection.	Ĭ		
CRITICAL	Apache Double Encoded Null Byte Vulnerability CVE-2020+1576 detected. Apply the Apache visconfig.jar hotfix in Adobe Security Notice aps009-12 More Information: http://www.adobe.com/support/securits/aps009-12.html Note Information: http://www.adobe.com/support/securits/aps009-12.html			
IMPORTANT	RDS is Enabled RDS should not be enabled on a production server.			
WARNING	.SON Prefix is disabled The Prefix serialized /SON with: // setting is not enabled in the ColdFusion Administrator. This is recommended for preventing JSON hipacking.			
WARNING	Server Header Version Disclosure The HTTP Server header is disclosing the following: Apache/2.2.11 (Unix) mod_ssl/2.2.11 (pen5)./0.9.7) dwn/2.dkm/4.dk. This information may allow an attacker, or script kieldle to easily identify your server as vulnerabilities become known for the version you are using. Home information: https://pense.patia/vallan.com/them/stl8.cfm.	1		
_				
<u> </u>	Book Schemelter Star (Lanas addates a consistent STS cite.			
	Server Newton Discinture The HTTP Server beaker is disclaming the following: Apache/2.2,11 d/mio mod_361/2.2,11 Open53.0,9.7, David 2, The Arthreader may allow an attacker, an script loade to easily identify your server at vulnerabilities become known for the version you are using.			
TALCOLUMN .	AND IN DOMESTIC			



Web Application Firewall for ColdFusion <u>http://foundeo.com/security/</u>



Wednesday, August 4, 2010

Thanks. Questions? pete@foundeo.com

<u>www.hackmycf.com</u> <u>www.foundeo.com</u>



Wednesday, August 4, 2010