LOCKING DOWN THE #COLDFUSION ADMINISTRATOR
YOUR FIRST LINE OF DEFENSE AGAINST HACKERS

Charlie Arehart
Independent Consultant

charlie@carehart.org / @carehart

Updated June 13, 2013
OUTLINE

• Introducing the challenge (recent attacks, fixes, “zero-day” concept)
• The key thing you can do to protect against most attacks
• How to lock down the CF Administrator (several approaches)
• Gotchas
  • Why locking down the entire CFIDE may be wrong
  • How protecting sites having CFIDE folder is not enough!
  • And more
• Finding evidence of / remediating past break-ins
• Resources
ABOUT CHARLIE AREHART

Independent Consultant

- 15 yrs CF experience (30 in Enterprise IT)
- Certified Adv CF Developer, Instructor
- Adobe Forum MVP, CF CAB member
- Frequent speaker to conf’s worldwide
- Organizer, Online ColdFusion Meetup (coldfusionmeetup.com), 2800+ members
- Living in Alpharetta, Georgia (Atlanta)

Web home at www.carehart.org

- 100+ presentations, 80+ articles, 400+ blog entries
- UGTV: recordings of 600+ presos by 300+ speakers
- CF411.com: 1800+ tools/resources, 150+ categories
- CF911.com: CF server troubleshooting resources
- Hosting courtesy of EdgeWeb Hosting
- Consulting: available for CF troubleshooting, tuning
  - Remote or on-site; on-demand, single instance is ok
INTRODUCING THE CHALLENGE

- The recent spate of attacks on CF servers
  - Some even made national news
  - Most significant (Dec/Jan) leveraged AdminAPI vulnerability
- More:
  - My 3 blog entries on the attack, the fixes
    - http://www.carehart.org/blog/client/index.cfm/2013/1/
  - Adobe fix that addressed it, and other fixes since
  - Understanding “zero-day” concept
THE KEY THING YOU CAN DO TO PROTECT AGAINST MOST ATTACKS

- What’s the number one thing you can do?
  - Might even argue it’s more important than CF hotfixes
- Locking down the CF Admin from public access
  - Note: this is NOT about whether CF Admin prompts for login
  - If your CF Admin login page is open to the public, you are vulnerable
- Protecting this would stop most of the recent attacks
- Protects even if you fail to apply updates / fail to apply them correctly
- Protects even if on CF8, for which Adobe provides no more updates
THE KEY THING YOU CAN DO TO PROTECT AGAINST MOST ATTACKS (CONT.)

• Is something Adobe has warned of for years (since at least CF8)
  • Documented in CF10, CF9 lockdown guide; CF8 Dev Sec Guide
  • Links to these offered later

• Really about locking down more than just the Admin. Other folders:
  • CFIDE/administrator
  • CFIDE/adminapi
    • This does not affect calls to AdminAPI by CF Admin or from within CFML
  • CFIDE/componentutils
  • CFIDE/wizards
  • And more
THE KEY THING YOU CAN DO TO PROTECT AGAINST MOST ATTACKS (CONT.)

• Beware CF Admin may be accessible many ways
  • Through more than one site in external web server
  • Through domains/ip addresses you may not consider
  • Through internal web server

• Quick demos

• While my experience is mainly with IIS and that’s what I’ll demo
  • Nearly all concepts / solutions apply to Apache, Nginx
HOW TO LOCK DOWN THE CF ADMINISTRATOR

• Several approaches available
  • Some apply to one web server or another
  • May choose more than one within a given web server
• Can lock down via
  • IP address
  • Web server authentication
  • IIS Request Filtering (IIS and Apache)
  • Scripting
• Lock down solutions I don’t recommend
TIP BEFORE ATTEMPTING TO LOCKDOWN

• Before attempting lockdown, be sure to first open the CF Admin however you normally would
  • Whether on the server or off it, whether using CF’s internal web server or your preferred external web server (IIS, Apache)
    • to ensure it still works when lockdown added
  • Then also open Admin in another browser or on another server, such as which you’d like to show would be locked down when done
    • To confirm first that it’s not, then later that it is, locked down
LOCKING DOWN ADMIN VIA IP ADDRESS

- At least two choices:
  - Limiting access to Admin folder to a given IP / set of them
  - Create/bind an admin-only site, to respond only on a given IP
- ...
LOCKING DOWN ADMIN VIA IP ADDRESS (CONT.)

- Approach 1: Limiting access to Admin folder by IP address
  - Done using site>properties>directory security in IIS 6
  - Done using “IP Address & Domain Restrictions” feature in IIS 7/8
    - Feature must be configured in (added as “role” to) server
      - See Lockdown Guide section on IIS Server Roles
    - Done at level of CFIDE/administrator folder, not at site level
    - Beware: don’t just add “deny entries” but also change “edit feature setting” to change default access from “allow” to “deny”
  - Done using Apache httpd.conf directives
  - Resources for IIS and Apache on next page
- Quick Demo of IIS
LOCKING DOWN ADMIN VIA IP ADDRESS (CONT.)

• CF Lockdown Guide
  • For Apache, “Prerequisites for a RedHat Enterprise Linux…”
  • For IIS, does not show ip limitation at folder level…

• Other resources:
  • http://toastergremlin.com/?p=185
  • http://serverfault.com/questions/136742/iis-7-5-limit-folder-access-to-local-users
  • http://tisupport.fr.yuku.com/topic/176
LOCKING DOWN ADMIN VIA IP ADDRESS (CONT.)

- Approach 2: Bind admin site to respond only on a given IP
  - See Lockdown Guide for details
    - For 10 Guide, “Create a Website For ColdFusion Administrator”
    - For 9, “Create the ColdFusion administrator website”
LOCKING DOWN ADMIN VIA WEB AUTHENTICATION

- Default access in web servers for any file/folder is “anonymous” access (anyone can see), so anyone can see the CF Admin login page
- Better choice:
  - Windows/NTLM Authentication
    - Safe to do over web (Basic auth is not)
- Quick Demo
- For more:
  - CF Lockdown Guide
    - For Apache, “Prerequisites for a RedHat Enterprise Linux…”
    - For IIS, see same section as on last slide
  - http://www.iis.net/configreference/system.webserver/security/authentication/windowsauthentication
LOCKING DOWN ADMIN VIA REQUEST FILTERING – IIS

- New feature in IIS 7 (not available for IIS 6)
  - Can block requests for any specific URL, path (or http verb, file extension, more)
- Need to install/enable at server level, even on IIS 7.0 / 7.5 / 8
  - See Lockdown Guide section on IIS Server Roles
- Could block access to Admin server-wide, then open it in desired site
- Quick Demo
- Beware that tool does not verify that the URLs you enter (to block) are valid
LOCKING DOWN ADMIN VIA REQUEST FILTERING
– IIS

• Lack of UI in IIS 7.0. Must enter XML
  • In applicationhost.config to control at server level
    • In C:\Windows\System32\inetsrv\config
  • In web.config to control at site level
    • In site docroot
  • See code on next slide for example (also resources, to follow)

• There is an extension to add the UI in 7.0
  • http://blogs.msdn.com/b/carlosag/archive/2008/03/24/iisadminpackrequestfiltering.aspx
  • http://blogs.msdn.com/b/carlosag/archive/2008/03/24/iisadminpackreuestfiltering.aspx
LOCKING DOWN ADMIN VIA REQUEST FILTERING – IIS (CONT.)

```xml
<requestFiltering>
  <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/portlets"/>
    <add sequence="/CFIDE/probe.cfm"/>
    <add sequence="/CFIDE/services"/>
    <add sequence="/CFIDE/wizards"/>
    <add sequence="/CFIDE/ServerManager"/>
    <add sequence="/CFIDE/scripts"/>
  </denyUrlSequences>
</requestFiltering>
```
LOCKING DOWN ADMIN VIA REQUEST FILTERING – IIS (CONT.)

• More:
  • CF Lockdown Guide
    • For 10
      • “Setup Request Filtering”
      • “Remove Request Filtering Rule for ColdFusion Administrator Site”
    • For 9, “Block /CFIDE requests”
  • http://www.petefreitag.com/item/741.cfm
LOCKING DOWN ADMIN VIA REQUEST FILTERING
- APACHE

• Could block via Apache conf

```html
<Location CFIDE/administrator>
Order Deny,Allow
Deny from All
Allow from 127.0.0.1
</Location>
```

• More:
  • CF Lockdown Guide, in section “Prerequisites for a RedHat Enterprise Linux…”
  • http://www.aaronwest.net/blog/index.cfm/2010/10/4/Blocking-ColdFusion-Administrator-in-Apache

• Could also use mod_rewrite
LOCKING DOWN ADMIN VIA SCRIPTING

- Valuable if you have multiple sites / servers to secure
- In IIS 7, can use appcmd tool (in C:\Windows\System32\inetsrv\)
  - or powershell
  - Or ADSI, WMI, and more
- Resources:
  - http://www.iis.net/learn/manage/powershell
A TIP: REQUIRING SSL FOR CF ADMIN

• While not about locking down public access, another good practice would be to require SSL for accessing the CF Admin
  • For more, on both Apache and IIS, see:
  • http://www.petefreitag.com/item/725.cfm
SOLUTIONS I DON’T RECOMMEND

• Some “lockdown” by locking down ENTIRE CFIDE
  • Will explain in next section why I don’t recommend that

• Some “lockdown” by removing CF admin entirely
  • They literally delete (or rename) the CF Admin (or CFIDE) to “remove” it
    • And they return/rename it when they want to access Admin
  • Just seems less desirable when other solutions exist

• Some propose “lockdown” by adding CFABORT to application.cfm of CFIDE/administrator
  • But some hacks were not via CFIDE/administrator but adminapi
  • Also, admin’s application.cfm is encoded, not editable
GOTCHAS

• How locking down the Admin alone is not enough (discussed)
• Why locking down the entire CFIDE may be wrong
• How more than one site/domain/IP may serve CF Admin
• How protecting sites having CFIDE folder is not enough!
WHY LOCKING DOWN THE ENTIRE CFIDE MAY BE WRONG

• Several CFIDE subfolders are used by apps, features
  • Scripts, portlets, services, orm, debug, componentutils, air
  • Scripts used by not only java applets, cfform cfgrid, and flash forms
    • But also Ajax features and much more
• There are also some URLs served via CFIDE that don’t really exist there
  • /CFIDE/graphdata, /CFIDE/main/ide.cfm (for RDS)
• If locking down, confirm if these still respond, for example:
  • /CFIDE/images/required.gif
  • :/CFIDE/scripts/ajax/resources/ext/images/default/tabs/xd-tab-strip-bg.gif
WHY LOCKING DOWN THE ENTIRE CFIDE MAY BE WRONG (CONT.)

- When troubleshooting these issues, can be helpful to use browser proxy / http sniffer tools
  - http://www.carehart.org/blog/client/index.cfm/2012/3/20/builtin_browser_proxy_sniffer_tools
- May want to check your web server logs for 404/403s on /CFIDE/scripts calls
- Another option: can redefine the scripts location to outside of CFIDE
  - Then it’s vital to create real or virtual dir in web server (or Alias directive in Apache) for all sites that may need scripts
  - But then could lock down “all of CFIDE” for other than Admin use
- More: http://www.petefreitag.com/item/774.cfm
HOW MORE THAN ONE SITE/DOMAIN/IP MAY SERVE CF ADMIN

• Understanding binding of sites to domain(s)/IP(s)
• Understanding “default site” (in IIS)
  • How (by default) it handles any domains/IPs not bound to other sites
• Why some suggest (as does lockdown guide) creating cfadmin site
• Beware that CF10 connector adds CFIDE virtual directory to sites
HOW PROTECTING SITES HAVING CFIDE FOLDER IS NOT ENOUGH!

• Problem:
  • Even in a site without CFIDE (real or virtual directory / alias)
  • CF Admin login page may appear if requested
    • (unless you have added global request filtering, of course)

• How?
  • By default, when page is requested, looks first in web site docroot, THEN in [CF]wwwroot!
    • If CFIDE exists in [CF]wwwroot, it will be served!

• Is created either of two ways
  • If no external web server is selected at install
  • When (in CF Enterprise/Trial/Developer) a new instance is created

• Should just test all sites for whether admin is exposed
HOW PROTECTING SITES HAVING CFIDE FOLDER IS NOT ENOUGH! (CONT.)

- Fortunately, the request filtering features would block this
- If you want to lock down by IP or web auth
  - Not about locking down the internal web server’s access to CFIDE
  - Instead, may want to add a CFIDE VD where “not needed”, then lock it down by IP or web auth
- See “A real gotcha: implicit access to the built-in web server root” in http://www.carehart.org/blog/client/index.cfm/2013/1/2/Part2_serious_security_threat
- For me: confirm if it’s about the CF internal web server being enabled or not
  - (and update blog entry if so)
FINDING EVIDENCE OF / REMEDIATING PAST BREAK-INS

- Focus so far on how to protect, but what about determining if you were hit?
- Look in web server logs (or CF10 access logs)
  - For attempts to access
    - /CFIDE/adminapi
    - /CFIDE/componentutils
    - h.cfm, i.cfm, etc.
    - /CFIDE/scripts/ajax/FCKeditor/editor/filemanager/connectors/cfm/connector.cfm
    - others
- Tools to help do that
  - FileLocator Lite, wingrep, grep, editor file search features, etc.
FINDING EVIDENCE OF / REMEDIATING PAST BREAK-INS (CONT.)

• Note if status code is 200, 404, 403, or something else
  • Note that 200 may not necessarily mean page was served
  • For calls to h.cfm (and the like) look at fuseaction for things done
  • More at http://www.carehart.org/blog/client/index.cfm/2013/1/2/Part2_serious_security_threat

• Beware looking only in logs for sites you “think” may be vulnerable
• Beware that some sites may not do logging at all
  • All the more reason to look to CF10 access logs, or FusionReactor logs
• …
FINDING EVIDENCE OF / REMEDIATING PAST BREAK-INS (CONT.)

- Look on server for any unexpected scheduled tasks
  - Bad guys tended to create (and delete) a cfprobe sched task
  - Could look in scheduler.log for calls to that task
  - Could look in http.log (since 9.0.1)
    - to see calls from that sched task to remote page which returned CFML that was saved to file and then executed remotely
- Look on server in /CFIDE folder for any unexpected files
  - Bad guys tended to create h.cfm, help.cfm, etc.
  - You can execute the h.cfm file to see what it exposes (requested “code” is within file)
    - But don’t leave the file in a public directory with its given name: protect or delete it
FINDING EVIDENCE OF / REMEDIATING PAST BREAK-INS (CONT.)

• Look through server code base (all directories) for unexpected files
  • Could be cfm or exe files
  • They may have set the file modified date to past, to trick you
  • Best: compare to version control, local copy, dev server, etc.
• Do beware if moving to new system that you don’t bring compromised files
• Could also use an intrusion detection system
  • Or roll your own in CFML
    • http://www.dcepler.net/post.cfm/file-integrity-checking-cfide
    • https://github.com/dcepler/cfide-integrity
    • http://boncode.blogspot.com/2013/01/cf-scheduled-task-security-vulnerability.html
FINDING EVIDENCE OF / REMEDIATING PAST BREAK-INS (CONT.)

• May want to seriously consider locking down dirs that CF can access
  • Either by changing the user CF runs under, then restricting what dirs that user can access
  • Or by turning on the Resource Security / Sandbox Security feature in CF to limit what folders CFML code can touch
    • In Enterprise, Sandbox Security lets you control that per app
  • For more, see Lockdown Guide
• Also my Adobe Security Center articles on Sandbox/Resource Security
  • http://www.carehart.org/articles/#2002_11
  • http://www.carehart.org/articles/#2002_10
POST-MORTEM

• Some may ask
  • “Why hasn't Adobe done more to protect CF?“

• They have done quite a bit
  • The lockdown guides (for 9 and 10) and Dev Sec Guide (for 8) have long warned of need to lock down CF Admin
    • They’ve not done it for you, since you could configure many ways
  • And lockdown guide covers far more (now up to 80+) pages in CF10
    • Sadly, many have ignored the lockdown guide
  • They added “secure profile” in CF10, and have added still more security tweaks in 9 and 10 (separate from that)
    • http://www.adobe.com/devnet/coldfusion/articles/security-improvements.html
  • They have been updating CF more frequently recently (pro/con)
• How can I know if I am vulnerable? …
POST-MORTEM (CONT.)

- Check out hackmycf.com, from Pete Freitag and Foundeo
  - Free and commercial editions
  - Check for whether your CF Admin (and other vulnerable resources) are exposed
- Just beware: only checks the sites you tell it to check
  - Remember my warning that you may have sites that DO respond to Admin request that you may not think of
  - This tool will not detect/test those (currently)
  - Still, I do highly recommend the tool to use against your sites
- Of course, much more you could lockdown/secure with CF
  - Pete wrote the tool and the lockdown guide, will point to more you can do
  - And there is still more Adobe could do about CFIDE lockdown...
Let’s hope all this is addressed CF11 (or perhaps sooner). Adobe…

- Could separate scripts from CFIDE, so all CFIDE could be locked down
- Could prompt during install for domains/IPs on which admin should reply
  - Perhaps option to allow access to Admin only from on server itself
- Does already offer an option to limit IPs from which admin access is allowed
  - Applies to access via internal or external web server
  - Seems to always allow access from server itself, regardless
  - Does not require restart of CF to take effect
RESOURCES

• CF10, CF9 lockdown guides

• CF8 Dev Sec Guide
  • http://forta.com/blog/index.cfm/2013/1/14/Is-It-Safe-To-Block-Access-To-cfide
  • My 3 blog entries on the attack, the fixes
    • http://www.carehart.org/blog/client/index.cfm/2013/1/
    • http://www.michaels.me.uk/post.cfm/securing-your-coldfusionmx-installation-on-windows
      • While written for CF7, still applies (and shows this idea is not new)
RESOURCES (CONT.)

• Still others have talked about locking down CFIDE over the years
  • http://www.talkingtree.com/blog/index.cfm/2005/7/20/SecureAdmin
  • http://www.morgankelsey.com/post/how-to-lock-down-cfide-in-iis
  • http://www.aaronwest.net/blog/index.cfm/2010/10/4/Blocking-ColdFusion-Administrator-in-Apache
  • http://www.petefreitag.com/item/750.cfm
  • http://www.petefreitag.com/item/774.cfm
  • http://www.clarke.ca/post.cfm/coldfusion-administrator-lockdown
CONCLUSION

• Locking down the CF Admin is vital, in addition to CF hotfixes
  • Truly is first line of defense for most recent attacks
• Several ways to lock it down (ip, auth, filtering, more)
• Not enough to lock down only the CFIDE/Admin—other vital dirs
• Yet not wise to lock down ENTIRE CFIDE—esp. if scripts needed
• Not enough to protect ONLY sites with CFIDE dir, if CFIDE in cf wwwroot
• Finding evidence of / remediating past break-ins
• If you need help with these, I’m available to consulting
  • Remote or on-site, scheduled or on-demand, short-term
  • Satisfaction guaranteed or no payment expected