# 『二进制漏洞』精选帖分类索引

转载

weixin_30390075 于 2019-09-11 11:17:00 发布 578 收藏 4
文章标签： 人工智能 网络 运维
原文链接：http://www.cnblogs.com/csnd/p/11505185.html
版权
列表不定期更新，有遗漏的地方还望各位留帖补充:P
last update: 2019.04.05

---

从漏洞、漏洞利用、Fuzz、利用缓解四个方面总结的一张脑图
https://bbs.pediy.com/thread-216256.htm

『二进制漏洞分析』学习资源整理
https://bbs.pediy.com/thread-221851.htm

---

## 基础知识：

Windows格式化字符串漏洞利用
https://bbs.pediy.com/thread-132554.htm

Windows下的shellcode剖析浅谈
https://bbs.pediy.com/thread-99007.htm

通过hash值计算API的名字
https://bbs.pediy.com/thread-55187.htm

Shellcode编写之hash式函数调用及相关
https://bbs.pediy.com/thread-58393.htm

开发通用的shellcode在win10系统下测试的问题
https://bbs.pediy.com/thread-246532.htm

一份shellcode的详细分析
https://bbs.pediy.com/thread-46068.htm

Flash漏洞所用shellcode的分析
https://bbs.pediy.com/thread-65907.htm

CVE-2010-1297漏洞shellcode简析
https://bbs.pediy.com/thread-121236.htm

一个Word溢出样本的shellcode分析
https://bbs.pediy.com/thread-130249.htm

Egg Hunting - Shellcode分段执行技术原理
https://bbs.pediy.com/thread-129086.htm

一种反检测的Shellcode GetPC方法Flush GetPC
https://bbs.pediy.com/thread-154689.htm

Shellcode In x64
https://bbs.pediy.com/thread-155336.htm

缓冲区溢出攻击浅析，写给初学者
https://bbs.pediy.com/thread-131340.htm

堆溢出精髓分析与实践
https://bbs.pediy.com/thread-102527.htm

---

## CTF Pwn：

[新手向] 一步一步学pwntools
https://bbs.pediy.com/thread-247217.htm

HITB GSEC WIN PWN BABYSTACK分析
https://bbs.pediy.com/thread-221016.htm

从BookWriter看house_of_orange原理
https://bbs.pediy.com/thread-223334.htm

CTF堆利用：House Of Force
https://bbs.pediy.com/thread-222924.htm

堆溢出-House of orange 学习笔记
https://bbs.pediy.com/thread-222718.htm

ctf中 可执行文件patch技术
https://bbs.pediy.com/thread-222623.htm

如何在pwn题中更有效地使用GDB
https://bbs.pediy.com/thread-223337.htm

协程切换的临界区块控制不当而引发的UAF血案
https://bbs.pediy.com/thread-224686.htm

强网杯出题思路-solid_core-HijackPrctl
https://bbs.pediy.com/thread-225488.htm

printf函数leak与canary绕过原理及利用方式
https://bbs.pediy.com/thread-229447.htm

unlink 系列
https://bbs.pediy.com/thread-247007.htm

堆的六种利用手法
https://bbs.pediy.com/thread-246786.htm

Tcache利用总结
https://bbs.pediy.com/thread-249713.htm

Linux PWN从入门到熟练
https://bbs.pediy.com/thread-248682.htm

Linux PWN从入门到熟练（二）
https://bbs.pediy.com/thread-248681.htm

新手玩转Linux Kernel漏洞之Null Pointer Dereference
https://bbs.pediy.com/thread-227019.htm

linux kernel pwn 分析(一) 强网杯core + ciscn babydriver
https://bbs.pediy.com/thread-247054.htm

linux kernel pwn笔记
https://bbs.pediy.com/thread-247949.htm

---

## Mitigation Bypass：

Windows溢出保护原理与绕过方法概览
https://bbs.pediy.com/thread-123572.htm

二进制漏洞利用中的ROP技术研究与实例分析
https://bbs.pediy.com/thread-221041.htm

ROP【二进制学习】
https://bbs.pediy.com/thread-246484.htm

利用SEH异常处理机制绕过GS保护
https://bbs.pediy.com/thread-223443.htm

利用Stack Pivot和ROP绕过ASLR+DEP学习笔记
https://bbs.pediy.com/thread-146321.htm

Heap Spray技术要点
https://bbs.pediy.com/thread-156991.htm

JavaScript中的堆风水
https://bbs.pediy.com/thread-55879.htm

JIT Spray：利用JIT在内存中构造可控可执行代码
https://bbs.pediy.com/thread-109060.htm

MS08-067通用bypass DEP的缓冲区溢出栈帧构造方法的学习
https://bbs.pediy.com/thread-81667.htm

关于safeSEH和/GS技术
https://bbs.pediy.com/thread-134754.htm

利用msvcr71.dll与mona.py实现通用绕过DEP/ASLR
https://bbs.pediy.com/thread-139241.htm

SafeSEH和DEP都开启了，有办法破吗
https://bbs.pediy.com/thread-137468.htm

缓冲区溢出漏洞exploit在当下遇到的绝境
https://bbs.pediy.com/thread-179658.htm

Advanced Exploitation Technology Analyze
https://bbs.pediy.com/thread-192049.htm

分析微软EMET工具的两个功能实现
https://bbs.pediy.com/thread-125470.htm

野外的CVE-2015-2545逃逸了EMET
https://bbs.pediy.com/thread-216046.htm

EMET5.1绕过方法学习笔记
https://bbs.pediy.com/thread-199061.htm

Win10下EMET 5.5防护机制之Memport的绕过
https://bbs.pediy.com/thread-208774.htm

linux漏洞缓解机制介绍
https://bbs.pediy.com/thread-226696.htm

Windows 10 内核漏洞利用防护及其绕过方法
https://bbs.pediy.com/thread-227102.htm

---

## 图像漏洞：

Exploit for ANI file
https://bbs.pediy.com/thread-42208.htm

Microsoft TIFF图像文件处理栈溢出漏洞(MS07-055)
https://bbs.pediy.com/thread-57730.htm

认识PNG文件格式
https://bbs.pediy.com/thread-75181.htm

Adobe PDF LibTiff Integer Overflow CVE-2010-0188初探
https://bbs.pediy.com/thread-109316.htm

---

## Flash漏洞：

手把手一起分析最新Flash样本
https://bbs.pediy.com/thread-147686.htm

Adobe flash漏洞之CVE-2009-1862初探 -- 基础知识篇
https://bbs.pediy.com/thread-101342.htm

CVE-2011-0611分析
https://bbs.pediy.com/thread-137922.htm

CVE-2012-0769, the case of the perfect info leak
https://bbs.pediy.com/thread-155034.htm

Analysing the PoC of CVE-2012-0769
https://bbs.pediy.com/thread-149338.htm

CVE-2012-1535 Flash解析特殊格式字体漏洞样本构造分享
https://bbs.pediy.com/thread-157851.htm

CVE-2012-1535漏洞调试分析
https://bbs.pediy.com/thread-154860.htm

CVE-2012-1535 Flash漏洞调试笔记
https://bbs.pediy.com/thread-155101.htm

Adobe Flash Player远程代码执行漏洞分析（CVE-2012-1535）
https://bbs.pediy.com/thread-156124.htm

CVE-2013-0634 PoC Analysis
https://bbs.pediy.com/thread-162493.htm

CVE-2014-0322完整详细分析
https://bbs.pediy.com/thread-193313.htm

CVE-2015-3090 Exploit利用分析
https://bbs.pediy.com/thread-202461.htm

New Flash Exploition Analysis
https://bbs.pediy.com/thread-199166.htm

Flash漏洞利用样本逆向分析艺术
https://bbs.pediy.com/thread-215882.htm

Flash 0day(CVE-2018-4878)分析记录
https://bbs.pediy.com/thread-224527.htm

CVE-2018-15982漏洞分析报告
https://bbs.pediy.com/thread-248272.htm

---

## 网络协议漏洞：

MS08-067漏洞分析
https://bbs.pediy.com/thread-75361.htm

EMM's MS08-067 exploit原理分析
https://bbs.pediy.com/thread-80416.htm

MS17-010 SMB 远程命令执行漏洞利用分析
https://bbs.pediy.com/thread-217745.htm

WannaCry勒索软件中“永恒之蓝”漏洞利用分析
https://bbs.pediy.com/thread-217734.htm

CVE-2015-2370之DCOM DCE/RPC协议原理详细分析
https://bbs.pediy.com/thread-248128.htm

---

## 浏览器漏洞：

CVE-2010-0249 IE极光漏洞深入分析
https://bbs.pediy.com/thread-247763.htm

Analysis CVE-2011-0065 Firefox 3.6.16 mChannel use after free vulnerability
https://bbs.pediy.com/thread-139044.htm

Firefox UAF漏洞利用：基于shared array buffers
https://bbs.pediy.com/thread-220038.htm

IE8 sc.txt exploit分析学习
https://bbs.pediy.com/thread-142917.htm

Analysing the PoC of CVE-2012-0003
https://bbs.pediy.com/thread-146055.htm

CVE-2012-1875: mshtml.dll Use-After-Free漏洞分析
https://bbs.pediy.com/thread-152240.htm

CVE-2012-1876 MSHTML.DLL堆溢出漏洞分析
https://bbs.pediy.com/thread-153363.htm

CVE-2012-1876 Exploit利用分析
https://bbs.pediy.com/thread-202089.htm

CVE-2012-1889 Win7 通过GUID加载dll库绕过ASLR+DEP
https://bbs.pediy.com/thread-247975.htm

CVE-2012-4792漏洞分析
https://bbs.pediy.com/thread-173147.htm

UAF漏洞分析之CVE-2012-4969
https://bbs.pediy.com/thread-206412.htm

CVE-2013-1347（IE8 UAF漏洞）分析
https://bbs.pediy.com/thread-174631.htm

CVE-2013-1347: IE CLayoutBlock更新错误导致UAF
https://bbs.pediy.com/thread-182085.htm

IE漏洞CVE-2013-2551分析-附poc
https://bbs.pediy.com/thread-173600.htm

CVE-2013-3893: SetMouseCapture UAF
https://bbs.pediy.com/thread-182083.htm

CVE-2013-3893 IE浏览器uaf漏洞利用
https://bbs.pediy.com/thread-217373.htm

CVE-2014-0322 0day Exploit分析
https://bbs.pediy.com/thread-184608.htm

CVE-2014-0322 IE与Flash结合利用 绕过ASLR+DEP
https://bbs.pediy.com/thread-248057.htm

How to use VBScript to turn on the God Mode?
https://bbs.pediy.com/thread-189224.htm

About CVE-2014-6332
https://bbs.pediy.com/thread-194744.htm

CVE-2014-6332学习笔记
https://bbs.pediy.com/thread-248310.htm

CVE-2014-6332 修改浏览器安全属性开启Godmode
https://bbs.pediy.com/thread-248273.htm

CVE-2015-6086 简要分析
https://bbs.pediy.com/thread-209825.htm

CVE-2016-0189 vbs脚本引擎损坏漏洞分析
https://bbs.pediy.com/thread-228371.htm

对CVE-2016-0199的简单分析
https://bbs.pediy.com/thread-212058.htm

CVE-2017-11802分析
https://bbs.pediy.com/thread-222519.htm

CVE-2018-8174漏洞复现调试笔记
https://bbs.pediy.com/thread-246741.htm

CVE-2018-8174 “双杀”0day 从UAF到Exploit
https://bbs.pediy.com/thread-248477.htm

“深入”探索CVE-2018-8174
https://bbs.pediy.com/thread-249933.htm

记一次CVE-2018-8373利用构造过程
https://bbs.pediy.com/thread-246327.htm

一个拼凑起来的CVE-2018-8373的EXP
https://bbs.pediy.com/thread-246660.htm

CVE-2018-8373分析与复现
https://bbs.pediy.com/thread-246940.htm

IE浏览器漏洞综合利用技术：堆喷射技术
https://bbs.pediy.com/thread-223106.htm

IE浏览器漏洞综合利用技术：UAF利用技术的发展
https://bbs.pediy.com/thread-223107.htm

浏览器漏洞攻防对抗的艺术
https://bbs.pediy.com/thread-211277.htm

---

## 文档型漏洞：

完整剖析Acrobat Reader - Collab getIcon universal exploiter之路
https://bbs.pediy.com/thread-98571.htm

Adobe reader 漏洞CVE-2009-4324初步分析
https://bbs.pediy.com/thread-104890.htm

CVE-2009-3459漏洞PoC分析
https://bbs.pediy.com/thread-102514.htm

CVE-2011-0611初探
https://bbs.pediy.com/thread-136907.htm

CVE-2013-0640漏洞利用分析 - 附PoC
https://bbs.pediy.com/thread-163035.htm

MS10-087从漏洞补丁到PoC
https://bbs.pediy.com/thread-195992.htm

CVE-2011-0104 Excel缓冲区溢出漏洞分析
https://bbs.pediy.com/thread-144387.htm

对CVE-2011-0978稳定利用的分析
https://bbs.pediy.com/thread-145971.htm

Analysis CVE-2011-0978 Microsoft Office Excel Axis Properties Record Parsing Buff
https://bbs.pediy.com/thread-138428.htm

CVE-2012-0158分析笔记
https://bbs.pediy.com/thread-160149.htm

CVE-2012-0158两种poc分析
https://bbs.pediy.com/thread-217890.htm

不死鸟之眼——CVE-2012-0158的常见利用姿势
https://bbs.pediy.com/thread-230001.htm

解读天书----漏洞利用中级技巧的分析
https://bbs.pediy.com/thread-184721.htm

CVE-2013-3906简要分析
https://bbs.pediy.com/thread-181216.htm

CVE-2014-1761分析笔记
https://bbs.pediy.com/thread-192351.htm

CVE-2014-4114 SandWorm沙虫漏洞分析报告
https://bbs.pediy.com/thread-193443.htm

CVE-2012-1856 Office ActiveX控件MSCOMCTL.OCX UAF漏洞分析
https://bbs.pediy.com/thread-223844.htm

CVE-2013-3906漏洞分析
https://bbs.pediy.com/thread-225993.htm

分析CVE-2015-1641的记录
https://bbs.pediy.com/thread-230289.htm

从CVE-2015-1642到Office ActiveX控件堆喷探究
https://bbs.pediy.com/thread-250071.htm

结合一个野外样本构造一个cve-2016-7193弹计算器的利用
https://bbs.pediy.com/thread-221792.htm

CVE-2017-11826 样本分析
https://bbs.pediy.com/thread-221995.htm

CVE-2018-4990 Acrobat Reader 堆内存越界访问释放漏洞分析
https://bbs.pediy.com/thread-226971.htm

对CVE-2018-4990漏洞的补充分析
https://bbs.pediy.com/thread-250449.htm

---

## 虚拟化漏洞：

VMware漏洞实例分析之一 - 共享文件夹目录遍历漏洞
https://bbs.pediy.com/thread-74064.htm

360MarvelTeam虚拟化漏洞第一弹 - CVE-2015-6815漏洞分析
https://bbs.pediy.com/thread-206983.htm

虚拟机逃逸 -- QEMU的案例分析系列
https://bbs.pediy.com/thread-218045.htm

x86 架构下的 Hypervisor 与虚拟机实现概览
https://bbs.pediy.com/thread-225218.htm

Hyper-V安全从0到1系列
https://bbs.pediy.com/thread-222624.htm

QEMU 与 KVM 虚拟化安全研究介绍
https://bbs.pediy.com/thread-224371.htm

CVE-2017-4901 VMware虚拟机逃逸漏洞分析
https://bbs.pediy.com/thread-248384.htm

---

## 字体漏洞：

千年等一回-Adobe Reader CoolType库TTF字体解析栈溢出漏洞分析
https://bbs.pediy.com/thread-121986.htm

对CVE-2011-3402的利用分析
https://bbs.pediy.com/thread-147274.htm

---

## 内核漏洞：

MS08-025 win32k.sys NtUserFnOUTSTRING Privilege Escalation Exploit
https://bbs.pediy.com/thread-63099.htm

MS08-066 Microsoft Ancillary Function Driver Elevation of Privilege exploit
https://bbs.pediy.com/thread-74811.htm

Windows Vista/7 内核提权NtGdiEnableEudc 0day漏洞分析
https://bbs.pediy.com/thread-125514.htm

放个MS11-011分析、逆向、利用、绕过的文档、源代码
https://bbs.pediy.com/thread-130487.htm

CVE-2011-1984 wins提权漏洞分析
https://bbs.pediy.com/thread-140612.htm

如何触发MS11-080
https://bbs.pediy.com/thread-143695.htm

CVE-2013-3660漏洞分析
https://bbs.pediy.com/thread-178154.htm

CVE-2014-1767 Afd.sys double-free 漏洞分析与利用
https://bbs.pediy.com/thread-194457.htm

CVE-2014-4113分析及Exploit逆向
https://bbs.pediy.com/thread-198194.htm

安装vm tools导致的蓝屏牵出的内核bug分析
https://bbs.pediy.com/thread-215684.htm

内核漏洞利用技术文章集合
https://bbs.pediy.com/thread-129143.htm

内核进击之旅--HEVD--stackoverflow
https://bbs.pediy.com/thread-225513.htm

基于 GDI 对象的 Windows 内核漏洞利用
https://bbs.pediy.com/thread-226448.htm

Windows 内核系列一: UAF基础
https://bbs.pediy.com/thread-247019.htm

Windows 内核系列二: cve-2015-0057
https://bbs.pediy.com/thread-247281.htm

CVE-2018-8120 两种利用方式学习
https://bbs.pediy.com/thread-230051.htm

cve-2018-8453分析及利用EXP编写
https://bbs.pediy.com/thread-249021.htm

---

## 杀软漏洞：

金山毒霸2011内核溢出漏洞
https://bbs.pediy.com/thread-120343.htm

瑞星全功能安全软件2011内核拒绝服务漏洞
https://bbs.pediy.com/thread-151241.htm

趋势科技 tmactmon.sys DOS漏洞分析(0day)
https://bbs.pediy.com/thread-158396.htm

微点主动防御 Mp110013.sys <= 1.3.10123.0 本地内核权限提升漏洞
https://bbs.pediy.com/thread-110851.htm

---

## 其它漏洞：

LNK快捷方式文件漏洞简要分析
https://bbs.pediy.com/thread-117232.htm

CVE-2014-9707-GoaHead堆溢出漏洞形成分析
https://bbs.pediy.com/thread-216966.htm

GOAhead CVE-2017-17562深入分析
https://bbs.pediy.com/thread-223793.htm

CVE-2017-7269 IIS6.0远程代码执行漏洞分析及Exploit
https://bbs.pediy.com/thread-216809.htm

CVE-2017-7269：IIS6.0远程代码执行漏洞逆向分析记录
https://bbs.pediy.com/thread-216967.htm

cve-2017-8464分析
https://bbs.pediy.com/thread-248701.htm

一种新的btis服务com组件漏洞利用方式,成功提权至system
https://bbs.pediy.com/thread-228829.htm

用VBoxDbg调试并理解单线程版脏牛（CVE-2016-5195）
https://bbs.pediy.com/thread-246024.htm

CVE-2017-5123 waitid本地提权分析
https://bbs.pediy.com/thread-247014.htm

CVE-2017-8890漏洞分析
https://bbs.pediy.com/thread-246220.htm

关于CVE-2017-8890的一点细节
https://bbs.pediy.com/thread-248463.htm

CVE-2017-8890 漏洞分析 原理篇
https://bbs.pediy.com/thread-249193.htm

CVE-2017-8890 漏洞利用（root ubuntu@kernel-4.10.0-19）
https://bbs.pediy.com/thread-249194.htm

Linux CVE-2017-16995整数扩展问题导致提权漏洞分析
https://bbs.pediy.com/thread-249033.htm

CVE-2017-1000367 分析与复现
https://bbs.pediy.com/thread-218260.htm

CVE-2018-6789 Exim Off-by-one漏洞分析
https://bbs.pediy.com/thread-225986.htm

CVE-2018-1000001 glibc realpath缓冲区溢出漏洞分析
https://bbs.pediy.com/thread-228678.htm

CVE-2018-3639 最新侧信道攻击详细分析，深入架构和微指令
https://bbs.pediy.com/thread-245988.htm

ubuntu 内核源码调试方法（双机调试）
https://bbs.pediy.com/thread-249192.htm

《漏洞战争》配套资料下载
https://bbs.pediy.com/thread-211573.htm

---

## Fuzzing：

软件安全测试（fuzz）之大家一起学1：fuzz platform架构
https://bbs.pediy.com/thread-75032.htm

软件漏洞挖掘Fuzz工具之三 - 入门篇
https://bbs.pediy.com/thread-69910.htm

文件Fuzz教程系列索引
https://bbs.pediy.com/thread-176420.htm

软件漏洞挖掘之一_SPIKE
https://bbs.pediy.com/thread-68516.htm

基于SKIPE的网络协议Fuzzing技术
https://bbs.pediy.com/thread-180619.htm

对ActiveX控件进行Fuzzing测试发掘漏洞
https://bbs.pediy.com/thread-156920.htm

Windows XP SP3 AFD.sys 本地拒绝服务漏洞的挖掘过程
https://bbs.pediy.com/thread-165917.htm

漏洞挖掘方法之静态扫描+经典栈溢出实例
https://bbs.pediy.com/thread-184409.htm

afl-fuzz源码情景分析，详细读码笔记
https://bbs.pediy.com/thread-218671.htm

honggfuzz漏洞挖掘技术深究系列
https://bbs.pediy.com/thread-247954.htm

漏洞挖掘技术之 AFL 项目分析
https://bbs.pediy.com/thread-249912.htm

内核fuzz技术系列(1)——trinity
https://bbs.pediy.com/thread-250302.htm

fuzzing技术总结
https://bbs.pediy.com/thread-248997.htm

关于 fuzz 的 一点总结
https://bbs.pediy.com/thread-249986.htm

---

## 技术专题：

软件漏洞分析入门
https://bbs.pediy.com/thread-56445.htm

二进制漏洞入门教程
https://bbs.pediy.com/thread-208596.htm

Exploit编写系列教程1-10合集
https://bbs.pediy.com/thread-123602.htm

Linux (x86) Exploit 开发系列1~12合集
https://bbs.pediy.com/thread-217390.htm

---

## 经验心得：

漏洞分析的那些事儿
https://bbs.pediy.com/thread-142265.htm

软件漏洞分析技巧分享
https://bbs.pediy.com/thread-185817.htm

众里寻他千百度----文件类漏洞ShellCode的查找
https://bbs.pediy.com/thread-121045.htm

简单谈谈Java Exploit
https://bbs.pediy.com/thread-143826.htm

调试AVM中的JITed code技巧
https://bbs.pediy.com/thread-194903.htm

漏洞挖掘之个人见解
https://bbs.pediy.com/thread-140597.htm

转载于：https://bbs.pediy.com/thread-221734.htm

转载于:https://www.cnblogs.com/csnd/p/11505185.html