

《漏洞战争》

图书基本信息

书名：《漏洞战争》

13位ISBN编号：9787121289806

出版时间：2016-7-1

作者：林垚泉

页数：604

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《漏洞战争》

内容概要

《漏洞战争：软件漏洞分析精要》系统地讲解软件漏洞分析与利用所需的各类工具、理论技术和实战方法，主要涉及Windows 和Android 系统平台。《漏洞战争：软件漏洞分析精要》根据不同的软件漏洞类型划分，比如堆栈溢出、沙盒逃逸、类型混淆、UAF、内核漏洞等，同时又针对当前流行的移动安全，加入Android 平台上的漏洞分析与利用。以精心挑选的经典漏洞为例，以分享漏洞的分析技巧和工具为主，对这些漏洞的成因、利用及修复方法进行详细讲解，旨在"授之以渔"。《漏洞战争：软件漏洞分析精要》最大的特点是以各种类型的经典漏洞作为实战讲解，摒弃空头理论，几乎是"一本用调试器写出来的书"。

《漏洞战争：软件漏洞分析精要》适合计算机相关专业的本科及研究生，信息安全爱好者，软件安全及移动安全相关的安全从业人员，软件开发与测试人员、黑客等阅读。

《漏洞战争》

作者简介

林桺泉，网络ID:riusksk、泉哥、林大夫，毕业于福建中医药大学中西医骨伤专业，大学期间曾在《黑客防线》发表安全技术文章30余篇，大五参加看雪学院主办、微软赞助的“微软杯”ExploitMe安全调试技术个人挑战赛，荣获二等奖；毕业后就职于腾讯安全应急响应中心（TSRC），主要从事安全应急响应工作，研究方向主要聚集在软件安全、移动安全、Web安全等方向。业余时间，偶尔帮助友商解决安全问题，曾获得微软、Adobe、Yahoo、百度、阿里、网易等大厂商的漏洞致谢。

书籍目录

第1章 基础知识 1

11 漏洞的相关概念 1

111 什么是漏洞 1

112 漏洞的价值 1

113 0Day 漏洞 2

114 PoC 与Exploit 2

12 为什么要分析漏洞 2

13 常用分析工具 3

131 IDA-反汇编利器 3

132 OllyDbg-破解与逆向常用调试器 4

133 Immunity Debugger-漏洞分析专用调试器 4

134 WinDbg-微软正宗调试器 5

135 GDB-Linux 调试器 6

136 JEB-Android 反编译器 7

137 其他 8

14 常见的漏洞分析方法 8

141 静态分析 8

142 动态调试 9

143 源码分析 9

144 补丁比较 9

145 污点追踪 10

15 学习资源 11

151 站点分享 11

152 书籍推荐 12

16 本章总结 13

第2章 栈溢出漏洞分析 14

21 栈溢出简史 14

22 栈溢出原理 15

23 CVE-2010-2883 Adobe Reader TTF 字体SING 表栈溢出漏洞 16

231 LuckyCat 攻击事件 16

232 漏洞描述 18

233 分析环境 18

234 基于字符串定位的漏洞分析方法 19

235 样本Exploit 技术分析 20

236 样本Shellcode 恶意行为分析 26

237 漏洞修复 29

24 CVE-2010-3333 Microsoft RTF 栈溢出漏洞 30

241 林来疯攻击事件 30

242 漏洞描述 31

243 分析环境 31

244 RTF 文件格式 32

245 基于栈回溯的漏洞分析方法 33

246 漏洞利用 41

247 Office 2003 与Office 2007 Exploit 通用性研究 42

248 漏洞修复 45

25 CVE-2011-0104 Microsoft Excel TOOLBARDEF Record 栈溢出漏洞 51

251 漏洞描述 51

- 252 分析环境 52
- 253 基于污点追踪思路的漏洞分析方法 52
- 254 漏洞修复 59
- 26 阿里旺旺ActiveX 控件imageMandll 栈溢出漏洞 60
- 261 漏洞描述 60
- 262 分析环境 60
- 263 针对ActiveX 控件的漏洞分析方法 60
- 264 漏洞利用 63
- 27 CVE-2012-0158 Microsoft Office MSCOMCTLocx 栈溢出漏洞 65
- 271 Lotus Blossom 行动 65
- 272 漏洞描述 65
- 273 分析环境 65
- 274 基于OffVis 工具的Office 漏洞分析方法 66
- 275 漏洞修复 71
- 28 总结 72
- 第3章 堆溢出漏洞分析 73
- 31 堆溢出简史 73
- 32 堆溢出原理 74
- 33 堆调试技巧 79
- 331 堆尾检查 80
- 332 页堆 81
- 34 CVE-2010-2553 Microsoft Cinepak Codec CVDecompress 函数堆溢出漏洞 85
- 341 漏洞描述 85
- 342 分析环境 85
- 343 基于HeapPage 的堆漏洞分析方法 85
- 344 漏洞修复 101
- 35 CVE-2012-0003 Microsoft Windows Media Player winmmdll MIDI 文件堆溢出漏洞 104
- 351 关于"蜘蛛"漏洞攻击包 (Zhi-Zhu Exploit Pack) 104
- 352 漏洞描述 105
- 353 分析环境 105
- 354 MIDI 文件格式 105
- 355 基于导图推算的漏洞分析方法 107
- 356 漏洞利用 122
- 357 补丁比较 130
- 36 CVE-2013-0077 Microsoft DirectShow quartzdll m2p 文件堆溢出漏洞 130
- 361 漏洞描述 130
- 362 基于HTC 的漏洞分析方法 131
- 363 漏洞修复 134
- 37 CVE-2012-1876 Internet Exporter MSHTMLdll CalculateMinMax 堆溢出漏洞 135
- 371 在Pwn2Own 黑客大赛上用于攻破IE9 的漏洞 135
- 372 分析环境 135
- 373 基于HPA 的漏洞分析方法 135
- 374 通过信息泄露实现漏洞利用 149
- 375 漏洞修复 161
- 38 小结 163
- 第4章 整数溢出漏洞分析 164
- 41 整数溢出简史 164
- 42 整数溢出原理 164
- 421 基于栈的整数溢出 165

- 422 基于堆的整数溢出 166
- 43 CVE-2011-0027 Microsoft Data Access Components 整数溢出漏洞 167
- 431 在Pwn2Own 黑客大赛上用于攻破IE8 的漏洞 167
- 432 基于堆分配记录的漏洞分析方法 168
- 433 补丁比较 176
- 44 CVE-2012-0774 Adobe Reader TrueType 字体整数溢出漏洞 178
- 441 漏洞描述 178
- 442 PDF 文件格式与常用分析工具 178
- 443 基于条件记录断点的漏洞分析方法 182
- 444 补丁分析 196
- 45 CVE-2013-0750 Firefox 字符串替换整数溢出漏洞 197
- 451 漏洞描述 197
- 452 基于源码调试的漏洞分析方法 197
- 453 源码比对 207
- 46 CVE-2013-2551 Internet Explorer VML COALineDashStyleArray 整数溢出漏洞 208
- 461 在Pwn2Own 黑客大赛上攻破IE10 的漏洞 208
- 462 基于类函数定位的漏洞分析方法 208
- 463 利用信息泄露实现漏洞利用 223
- 47 总结 226
- 第5章 格式化字符串漏洞分析 227
- 51 格式化字符串漏洞简史 227
- 52 格式化字符串漏洞的原理 227
- 53 CVE-2012-0809 Sudo sudo_debug 函数格式化字符串漏洞 234
- 531 漏洞描述 234
- 532 通过源码比对分析漏洞 234
- 54 CVE-2012-3569 VMware OVF Tool 格式化字符串漏洞 235
- 541 漏洞描述 235
- 542 基于输出消息的漏洞定位方法 235
- 543 漏洞利用 239
- 55 总结 242
- 第6章 双重释放漏洞分析 243
- 61 双重释放漏洞简史 243
- 62 双重释放漏洞的原理 243
- 63 CVE-2010-3974 Windows 传真封面编辑器fxscoverexe 双重释放漏洞 246
- 631 漏洞描述 246
- 632 通过栈回溯和堆状态判定漏洞类型 246
- 633 通过补丁比较确定漏洞成因及修复方法 249
- 64 CVE-2014-0502 Adobe Flash Player 双重释放漏洞 251
- 641 GreedyWonk 行动 251
- 642 静态分析攻击样本 251
- 643 Shellcode 自动化模拟执行 263
- 644 基于ROP 指令地址的反向追踪 265
- 65 总结 273
- 第7章 释放重引用漏洞分析 274
- 71 释放重引用 (Use After Free , UAF) 漏洞简史 274
- 72 UAF 漏洞的原理 274
- 73 CVE-2011-0065 Firefox mChannel UAF 漏洞 277
- 731 漏洞描述 277
- 732 通过动态调试快速定位漏洞源码 277

- 733 漏洞利用 285
- 734 源码比对 286
- 74 CVE-2013-1347 Microsoft IE CGenericElement UAF 漏洞 287
- 741 "水坑"攻击事件 287
- 742 通过HPA 快速定位漏洞对象 287
- 743 逆向分析IE 引擎对JavaScript 代码的解析 290
- 744 追本溯源：探寻漏洞的本质 321
- 745 漏洞利用 324
- 75 CVE-2013-3346 Adobe Reader ToolButton UAF 漏洞 326
- 751 "Epic Turla"网络间谍攻击行动 326
- 752 使用peepdf 分析PDF 恶意样本 326
- 753 漏洞利用 338
- 76 CVE-2015-0313 Adobe Flash Player Workers ByteArray UAF 漏洞 340
- 761 漏洞描述 340
- 762 分析ActiveScript 虚拟机源码辅助漏洞调试 340
- 763 Flash JIT 调试插件与符号文件 353
- 764 漏洞利用 354
- 765 漏洞修复 360
- 77 本章总结 360
- 第8章 数组越界访问漏洞分析 361
- 81 数组越界与溢出的关系 361
- 82 数组越界访问漏洞原理 361
- 83 CVE-2011-2110 Adobe Flash Player 数组越界访问漏洞 363
- 831 漏洞描述 363
- 832 解决安装旧版Flash Player 的限制问题 364
- 833 通过Perl 脚本辅助分析样本 365
- 834 搭建服务器重现漏洞场景 371
- 835 通过修改样本代码定位漏洞 373
- 836 通过构造信息泄露利用漏洞 376
- 837 通过搜索指令序列分析补丁 380
- 84 CVE-2014-0160 OpenSSL TLS 数组越界访问漏洞 ("心脏出血") 382
- 841 漏洞描述 382
- 842 基于源码对比与跟踪的漏洞分析方法 383
- 843 利用漏洞盗取网站账号 389
- 85 本章总结 394
- 第9章 内核漏洞分析 395
- 91 Windows 内核漏洞漫谈 395
- 92 Windows 内核调试环境搭建 396
- 93 常见内核漏洞原理与利用 398
- 931 漏洞成因分析 398
- 932 漏洞利用 405
- 94 360 安全卫士bregdrvsys 本地提权漏洞分析 414
- 941 漏洞描述 414
- 942 基于导出函数和IO 控制码的追踪分析 414
- 95 CVE-2011-2005 Windows Afdsys 本地提权漏洞 423
- 951 漏洞描述 423
- 952 从利用代码到漏洞函数的定位分析 423
- 953 补丁比较 426
- 96 CVE-2013-3660 Windows win32ksys EPATHOB 指针未初始化漏洞 426

- 961 漏洞描述 426
- 962 通过IDA 定义结构体辅助分析 427
- 963 漏洞利用 431
- 97 CVE-2014-1767 Windows AFDsys 双重释放漏洞 (Pwn2Own 2014) 437
- 971 Pwnie Awards 2014"最佳提权漏洞奖"得主 437
- 972 基于IOCTL 处理函数自动追踪记录的分析方法 437
- 973 漏洞利用 454
- 974 补丁分析 460
- 98 本章总结 462
- 第10章 Android 平台漏洞分析 463
- 101 Android 平台漏洞简史 463
- 102 Android 平台漏洞分类 466
- 103 常见的漏洞分析方法 467
- 1031 APK 静态分析 467
- 1032 smali 动态调试 468
- 1033 so 库动态调试 474
- 1034 补丁源码比对 475
- 1035 系统Java 源码调试 477
- 1036 系统C/C++源码调试 486
- 1037 Android 内核源码调试 488
- 104 智能插座漏洞分析 492
- 1041 漏洞描述 492
- 1042 静态逆向分析 492
- 1043 利用漏洞控制网络上的任意插座 497
- 1044 总结 502
- 105 CVE-2013-4787 Android 系统签名漏洞 502
- 1051 漏洞描述 502
- 1052 Android 签名机制 503
- 1053 漏洞重现 509
- 1054 漏洞原理分析 514
- 1055 漏洞修复 516
- 106 CVE-2010-1119 Android WebKit UAF 漏洞 516
- 1061 漏洞描述 516
- 1062 漏洞利用 517
- 1063 通过补丁源码分析漏洞成因 524
- 107 CVE-2014-3153 Android 内核Futex 提权漏洞 (Towelroot) 528
- 1071 Android 设备Root 神器-Towelroot 528
- 1072 通过内核源码调试分析漏洞 528
- 1073 漏洞利用 548
- 1074 漏洞修复 554
- 108 本章总结 554
- 第11章 其他类型的漏洞分析 555
- 111 本章引言 555
- 112 CVE-2013-2423 JAVA Applet reflection 类型混淆代码执行漏洞 555
- 1121 漏洞描述 555
- 1122 类型混淆漏洞 555
- 1123 Java 安全机制 556
- 1124 漏洞分析与利用 558
- 1125 漏洞修复 562

- 1126 2013 年漏洞之王-Java 563
- 113 CVE-2014-0257 Microsoft Internet Explorer 11 dfsvc 组件沙盒逃逸漏洞 564
- 1131 漏洞描述 564
- 1132 IE 沙盒保护原理 564
- 1133 IE 沙盒攻击面分析 569
- 1134 CVE-2014-0257 漏洞分析与利用 570
- 114 CVE-2014-9150 Adobe Acrobat Reader MoveFileEx IPC Hook 竞争条件 (沙盒逃逸) 漏洞 572
- 1141 Therac-25 医疗事故 572
- 1142 竞争条件漏洞原理 573
- 1143 CVE-2014-9150 漏洞描述 574
- 1144 Adobe 沙盒简介 574
- 1145 利用漏洞实现沙盒逃逸 575
- 115 本章总结 578
- 第12章 软件漏洞发展趋势 579
- 121 软件漏洞领域的新挑战 579
- 122 移动终端漏洞发展趋势 579
- 123 云计算平台漏洞发展趋势 581
- 124 物联网漏洞发展趋势 583
- 125 本章总结 585

《漏洞战争》

精彩短评

- 1、 还得读读汇编书籍才能看，这个比C++还天书
- 2、 riusk's blog 作者博客以及github在维护的一本书，讲究黑客方法，图书馆订购中，mark一下看不懂，但感觉不是很好
- 3、 很多地方还是太一带而过了，不如网上的文章写的好。

《漏洞战争》

精彩书评

1、这是一本内行人写的内行书，把很多前人的经验总结都写了进来。这本书更多的是以一种方法论的方式来向大家介绍软件漏洞分析，所以不必过于拘泥于细节。掌握方法更为重要。最后感谢泉哥能分享出这些经验，可以帮助后来者少走无数的弯路。

.....
.....
.....

《漏洞战争》

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu000.com