Google Project Zero挖洞经验整理

threatactor / 2017-01-15 13:55:05 / 浏览数 3541 安全技术 漏洞分析 顶(0) 踩(0)

---

1. 目标：漏洞挖掘越来越难
1. 关注客户端，包括安卓，IOS，WINDOWS操作系统，PDF,DOC,AV等等；各种OSS开源代码安全，并且开放了OSS-FUZZ工具；
1. 漏洞削减技术来帮助Google的技术提升，包括彻底修复一类漏洞、彻底修复这个漏洞，此种漏洞的攻击面、增加这个漏洞利用的阶段性必须使用组合技术绕过；
1. 漏洞挖掘方法：Fuzzing、优秀的漏洞挖掘者想出如何挖洞的思路、针对高难度的内核等需要手工（手工输出经验）；
1. 公开漏洞挖掘和使用的技术：
   https://github.com/google/oss-fuzz
   https://github.com/google?utf8=%E2%9C%93&q=fuzz&type=&language=\
   工具：valgrind
   公开设计方法：例如chrome的设计原则
   公开漏洞细节：https://googleprojectzero.blogspot.com/
   Fuzzing技术分成：
   a、内存Sanitizer：未初始化指针；
   b、地址Sanitizer:发现UAF、缓冲区溢出、内存泄露； Google 99%项目应用在单元测试；
   c、进程Sanitizer：发现竞争条件等漏洞；
   d、UBSanitizer：未知行为的；
1. 参考地址：
   https://www.youtube.com/watch?v=ZKIIPu1wqHs Google Project One
   https://www.youtube.com/watch?v=FP8zFhB_cOo Google Fuzzing
1. 发现漏洞列表:
   https://code.google.com/p/google-security-research/issues/detail?id=222
   https://bugs.chromium.org/p/project-zero/issues/list?can=1&q=&colspec=ID+Type+Status+Priority+Milestone+Owner+Summary&cells=ids
1. Google Fuzzing规模
   a、 24*7无间断的5000核CPU跑；
   b、5000+ bugs in chromium 1200+ bugs in ffmpeg；
   c、数百种fuzzing方式；
   d、高代码涵盖量；
   e、工具Libfuzzer:最典型的发现了OpenSSL心脏滴血漏洞；
   f、高效样本构造；
1. 详细细节（高端玩法Timeless debugger技术有点类似狼来了高端玩法狼自杀）
   工具：
   http://qira.me/
   https://github.com/BinaryAnalysisPlatform/qira

10.最终目标

Google是从设计框架规范、到单元测试、到漏洞挖掘深度和方式、到削减漏洞一条线的闭环。（纯漏洞角度，没有涵盖其他SDL原则和方法）

点击收藏 | 0 关注 | 0

上一篇：好多人问先知众测1月份还有没有月度奖励？ 下一篇：攻击JavaWeb应用[6]-程序...

1. 2 条回复


hades 2017-01-16 03:33:23

Fuzzing硬件的跟上。。。

0 回复Ta


笑然 2017-01-16 04:15:26

膜拜鸟哥

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