「 深蓝洞察 」2022 年度最“不可赦”漏洞

Original 深蓝 DarkNavy 2023-02-28 11:19 Posted on 上海

深蓝洞察

2022 年度
十大安全漏洞与利用
(十)

DARKNAVY 深蓝

2023 年 2 月

本篇为《深蓝洞察 | 2022 年度十大安全漏洞与利用》的第十篇。

认可白帽黑客价值、走进安全社区，打造安全团队，借助黑客视角提升自身安全能力，这已经成为了行业最佳安全实践之一。

但是，也有少数地下或隐蔽的公司通过招募黑客，用他们掌握的黑客技术寻找并利用漏洞，为自身牟取非法利益。

2022 年，竟有巨头公司打破底线，将白帽黑客作为武器，指向了用户。

2022 年，Google 的 Project Zero 发布了一个在野漏洞利用的分析，警告攻击者已经瞄准各手机厂商的 OEM 代码部分，挖掘出其中的脆弱点和漏洞，组合出了一套完整的提权攻击 Exploit。

Project Zero 分析的漏洞利用链包含四个部分，完全由三星代码中的漏洞组成。

第一步，攻击者利用了 漏洞 (CVE-2021-25337)，这是一个 system_server 中导出的 semclipboardprovider 所存在的任意文件读写，允许攻击者以 untrusted_app 身份读写 users_system_data_file，也就是一般 system_app 的私有数据文件。

第二步，攻击者参考了三星 TTS 漏洞研究成果，利用 TTS 中从自身配置文件加载任意动态链接库

的能力，将第一个漏洞转化为了一个 system_app 提权漏洞。

在获取了 system_app 权限的代码执行能力后，攻击者执行最后两步，向内核进发：

首先，将三星设备中未更新的 Mali GPU 驱动内核信息泄露漏洞 (CVE-2021-25369) ，和三星自己的 kmsg 泄露“特性”组合利用，最终获得内存基址和 addr_limit 地址。

然后，使用 DECON driver 中的 UAF 漏洞 (CVE-2021-25370)， 结合堆风水，最终，利用 signalfd 系统调用修改 addr_limit，转化为内核任意地址读写，完成提权。

至此，一套完整的提权攻击 Exploit 全部完成（上述攻击所涉及漏洞目前已全部修复）。

三星 OEM 漏洞攻击是一个很典型的案例，可以看出，与 AOSP、上游 Kernel 的漏洞挖掘难度相比，手机厂商 OEM 代码部分的漏洞挖掘难度要低很多，且利用通常也相当稳定。

于是我们经常可以看到，各种间谍软件的作者会频繁利用手机 OEM 代码漏洞作恶。

但 2022 年，有**知名互联网厂商竟持续挖掘新的安卓 OEM 相关漏洞，在其公开发布的 App 中实现对目前市场主流手机系统的漏洞攻击。**

以下技术分析和截图，均来自此刻正发生在数以亿计手机上的真实案例。相关敏感信息已经过处理。

该互联网厂商在自家看似无害的 App 里，使用的第一个黑客技术手段，是利用一个近年来看似默默无闻、但实际攻击效果非常好的 Bundle 风水 - Android Parcel 序列化与反序列化不匹配系列漏洞，实现 0day/Nday 攻击，从而绕过系统校验，获取系统级 StartAnyWhere 能力。

上下滑动查看案例相关代码

上图即是其漏洞利用链中的核心环节，利用了多个安卓手机厂商 OEM 代码中的反序列化漏洞，完成了第一步黑客攻击：提权。

完成了提权，该 App 事实上已经完成了反客为主，通过 App 控制了用户的整个手机系统。

> *Android Framework 中一个核心的对象传递机制是 Parcel，希望被通过 Parcel 传递的对象需要定义 readFromParcel 和 writeToParcel 接口函数，并实现 Parcelable 接口。*
> *理论上来讲，匹配序列化和反序列化函数应当是自反等效的，但系统 ROM 的开发者在编程过程中可能会出现不匹配的情况，例如写入的时候使用了 writeLong，读取的时候却使用了 readInt。*
> *这类问题在运行过程中一般不会引起注意，也不会导致崩溃或错误，但在攻击者精心布局下，却可最终利用 Settings 和 system_server 进程，将这个微小的错误转化为 StartAnyWhere 提权。*
> *Android 近年来累计已修复上百个这类漏洞，并在 Android 13 中对 Parcel 机制做了改革，彻底杜绝了大部分此类攻击面。*
> *但对于鸿蒙和绝大部分未升级到 Android 13 的设备和用户来说，他们仍处于危险之中。*

提权控制手机系统之后，该 App 即开启了一系列的违规操作，绕过隐私合规监管，大肆收集用户

的隐私信息（包括社交媒体账户资料、位置信息、Wi-Fi 信息、基站信息甚至路由器信息等）：

上下滑动查看案例相关代码

之后，该 App 进一步使用的另一个黑客技术手段，是利用手机厂商 OEM 代码中导出的 root-path FileContentProvider， 进行 System App 和敏感系统应用文件读写；

进而突破沙箱机制、绕开权限系统改写系统关键配置文件为自身保活，修改用户桌面(Launcher)配置隐藏自身或欺骗用户实现防卸载；

随后，还进一步通过覆盖动态代码文件的方式劫持其他应用注入后门执行代码，进行更加隐蔽的长期驻留；

甚至还实现了和间谍软件一样的遥控机制，通过远端“云控开关”控制非法行为的启动与暂停，来躲避检测。

上下滑动查看案例相关代码

最终，该互联网厂商通过上述一系列隐蔽的黑客技术手段，在其合法 App 的背后，达到了：

- 隐蔽安装，提升装机量
- 伪造提升 DAU/MAU
- 用户无法卸载
- 攻击竞争对手 App
- 窃取用户隐私数据
- 逃避隐私合规监管

等各种涉嫌违规违法目的。

目前，已有大量终端用户在多个社交平台上投诉反馈：该 App 存在莫名安装、泄漏隐私、无法卸载等问题。

这些行为不仅拉低了行业底线，破坏了公平竞争，更严重侵犯了用户的隐私，可能违反相关法律法规。

> *2021 年施行的《**网络产品安全漏洞管理规定**》第四条明确规定：“任何组织或者个人不得利用网络产品安全漏洞从事危害网络安全的活动，不得非法收集、出售、发布网络产品安全漏洞信息；明知他人利用网络产品安全漏洞从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。”*
> *在《**网络安全法**》、《**个人信息保护法**》中，对于此类行为也有针对性规定，并明确了相关法律责任。*
> *2 月 27 日，工信部发布了 **26 条措施**，聚焦 APP 安装卸载、服务体验、个人信息保护、诉求响应等，针对性地提出了改善措施；同时对 APP 开发运营者、分发平台、SDK（软件开发工具）、终端和接入企业细致地划分了责任。*

在手机设备复杂的供应链中，发现漏洞、修复漏洞、防范漏洞本就不易。

若还有巨头在名气的遮掩下利用漏洞牟利，将白帽变成黑帽，更会让用户和行业受伤。

我们在此呼吁，

一，手机厂商需要更重视自研代码的安全，削减不必要的、可能被攻击者利用的攻击面；

二，监管机构需要针对此类行为进行治理，根据现有法律法规严格执法、监管，严肃问责，以推进、构建一个更安全的数字环境。

个别公司的错误不该连带整个行业背负骂名，更不该由用户承担后果。

白帽也应当回归守护安全的初心，让技术发挥应有的正向作用。

参 考：

[1] https://googleprojectzero.blogspot.com/2022/11/a-very-powerful-clipboard-samsung-in-the-wild-exploit-chain.html

[2] https://xz.aliyun.com/t/2364

《2022 年度十大安全漏洞与利用》

结　语

最近几年，漏洞攻防技术变革节奏明显加快，这大大拉伸了攻防技能谱系。

在攻防对抗的末端，由于态度、方式不当或全局观、专业性欠缺等种种原因，我们依旧能看到脆弱不堪的防护机制和漏洞百出的系统、设备；
但在攻防对抗的最前沿，我们也会看到创新型、颠覆性攻击手法和机制性、深层逻辑型漏洞与日趋完善的纵深防御能力的精彩对抗。

这种环境下，漏洞研究人员更需要主动走出舒适区的勇气，保留好奇心，不断追求技术进步，发扬黑客精神，才能在攻防技术的最前沿做出新的成果。

扫码进 DarkNavy 官方交流群

你的洞见 群里见

Modified on 2023-03-02

People who liked this content also liked

简洁的chatGPT微信小程序(免费)

敲代码斯基

如何20元获得一台永久linux服务器

Drt安全战队

【漏洞通告】 Microsoft Word 远程代码执行漏洞（CVE-2023-21716）

绿盟科技CERT