

比葫芦娃还可怕的百度全系APP SDK漏洞 - WormHole虫洞漏洞分析报告

瘦蛟舞 (/author/瘦蛟舞) · 2015/11/02 10:50

作者：瘦蛟舞，蒸米

"You can't have a back door in the software because you can't have a back door that's only for the good guys." - Apple CEO Tim Cook

"你不应该给软件装后门因为你不能保证这个后门只有好人能够使用。" - 苹果CEO 库克

0x00 序

最早接触网络安全的人一定还记得当年RPC冲击波，WebDav等远程攻击漏洞和由此产生的蠕虫病毒。黑客只要编写程序扫描网络中开放了特定端口的机器，随后发送对应的远程攻击代码就可以控制对方主机，在控制对方主机后，程序可以继续扫描其他机器再次进行攻击。因为漏洞出在主机本身，想要修复漏洞必须安装补丁才行，但因为很多人并不会及时升级系统或者安装补丁，所以漏洞或者蠕虫会影响大量的机器非常长的时间，甚至有的蠕虫病毒可以感染全世界上亿的服务

器，对企业 and 用户造成非常严重的损失。

Android发布后，我们就一直幻想着能发现一个像PC上的远程攻击一样厉害的漏洞，但是Android系统默认并没有开放任何端口，开放socket端口的APP也非常稀少，似乎出现像PC那样严重的漏洞是不太可能的。但可惜的是，世界上并没有绝对的安全，就在这么几个稀少的端口中，我们真的找到了一个非常严重的socket远程攻击漏洞，并且影响多个用户量过亿的APP，我们把这个漏洞称之为WormHole虫洞漏洞。

0x01 影响和危害

WormHole虫洞漏洞到底有多严重呢？请看一下我们统计的受影响的APP列表（还没有统计全）：

百度地图 检测版本8.7
百度手机助手 检测版本6.6.0
百度浏览器 检测版本6.1.13.0
手机百度 检测版本6.9
hao123 检测版本6.1
百度音乐 检测版本5.6.5.0
百度贴吧 检测版本6.9.2
百度云 检测版本7.8
百度视频 检测版本7.18.1
安卓市场 检测版本6.0.86
百度新闻 检测版本5.4.0.0
爱奇艺 检测版本6.0
乐视视频 检测版本5.9
...完整列表见附录

这个列表是2015年10月14号统计的百度系APP的最新版，理论上所有小于等于检测版本的这些百度系的APP都有被远程攻击的危险。根据易观智库的统计排行：



(/author/瘦蛟舞)

瘦蛟舞 (/author/瘦蛟舞)

移动APPTOP200排名				
排名	APP名称	2015年04月 活跃用户数 (万)	2015年03月 活跃用户数 (万)	排名 对比
1	 微信	40850.63	40170.02	=
2	 QQ	30514.48	30493.14	=
3	 百度	15699.11	14878.65	=
4	 搜狗手机输入法	11305.44	11594.13	=
5	 淘宝	10832.94	10631.52	↑
6	 QQ浏览器	10668.16	10710.73	↓
7	 百度地图	9739.49	9722.85	=
8	 百度手机助手	9059.56	8556.75	↑
9	 UC浏览器	8986.02	8957.62	↓
10	 腾讯新闻	8784.69	8899.26	↓

drops.wooyun.org

可以看到手机百度、百度手机助手、百度地图等百度系APP有着上亿的下载安装量和加起来超过三亿的活跃用户。

安装了百度的这些APP会有什么后果和危害呢？

1. 无论是 wifi 无线网络或者3G/4G 蜂窝网络，只要是手机在联网状态都有可能受到攻击。攻击者事先无需接触手机，无需使用DNS欺骗。
2. 此漏洞只与app有关，不受系统版本影响，在google最新的android 6.0上均测试成功。
3. 漏洞可以达到如下攻击效果：
 - 远程静默安装应用
 - 远程启动任意应用
 - 远程打开任意网页
 - 远程静默添加联系人
 - 远程获取用户的GPS地理位置信息/获取imei信息/安装应用信息
 - 远程发送任意intent广播
 - 远程读取写入文件等。

下面是视频DEMO:

俺们做的视频效果太差,下面demo视频是从雷锋网上看到的：

<http://www.leiphone.com/news/201510/abTSIxRjPmIibScW.html>

0x02 漏洞分析

安装百度系app后，通过adb shell连接手机，随后使用netstat会发现手机打开了40310/6259端口，并且任何IP都可以进行连接。

```
public class ImmortalService
{
    private static final String ACTION_BIND = "com.baidu.hello.moplus.action.BIND";
    private static final boolean DEBUG = ;
    private static final short MAX_TRY_TIMES = 20;
    public static final String PARAMETER_CLASS = "class";
    public static final String PARAMETER_PACKAGE = "package";
    private static final String TAG = "ImmortalService";
    public static final String URI_DAEMON = "/daemon";
    public static final String URL_DAEMON = "http://127.0.0.1:40310/daemon?package=%s&class=%s";
    public static final String URL_MOPLUS = "http://127.0.0.1:40310";
    public static ServiceConnection sConnection = new a();
    private static Intent sRestartMoplus;
    private boolean isSetuping = false;
    private Context mContext;
    private boolean mIsBind = false;
    private boolean mIsServer = false;

    public ImmortalService(Context paramContext)
```

原来这个端口是由java层的nano http实现的，并且这个http服务，百度给起名叫immortal service（不朽/不死的服务）。为什么叫不朽的呢？因为这个服务会在后台一直运行，并且如果你手机中装了多个有wormhole漏洞的app，这些app会时刻检查40310/6259端口，如果那个监听40310/6259端口的app被卸载了，另一个app会立马启动服务重新监听40310/6259端口。



我们继续分析，整个immortal service服务其实是一个http服务，但是在接受数据的函数里有一些验证,比如 http 头部remote-addr字段是否是"127.0.0.1"，但是会一点web技巧的人就知道，只要伪造一下头部信息就可把remote-addr字段变成"127.0.0.1"。

```

FindFunc mFindFunc = new FindFunc(this.f);
if(TextUtils.equals(arg11.get("remote-addr"), "127.0.0.1")) {
    v0 = mFindFunc.a(mUri, arg10, arg11, arg12, arg13);
}
else if(TextUtils.equals(((CharSequence)mUri), "getcuid")) {
    v0 = mFindFunc.a(mUri, arg10, arg11, arg12, arg13);
}
else {
    goto label_115;
}

```

drops.wooyun.org

成功的和http server进行通讯后，就可以通过url给APP下达指令了。拿百度地图为例，以下是百度地图APP中存在的远程控制的指令的反汇编代码：

```

public class e
{
    private static final Map a = new HashMap();
    private static final String b = SendIntent.class.getPackage().getName() + ".";
    private Context c;

    static
    {
        a.put("geolocation", b + "GetLocLiteString");
        a.put("getsearchboxinfo", b + "GetSearchboxInfo");
        a.put("getapn", b + "GetApn");
        a.put("getserviceinfo", b + "GetServiceInfo");
        a.put("getpackageinfo", b + "GetPackageInfo");
        a.put("sendintent", b + "SendIntent");
        a.put("getcuid", b + "GetCuid");
        a.put("getlocstring", b + "GetLocString");
        a.put("scandownloadfile", b + "ScanDownloadFile");
        a.put("addcontactinfo", b + "AddContactInfo");
        a.put("getapplist", b + "GetApplList");
        a.put("downloadfile", b + "DownloadFile");
        a.put("uploadfile", b + "UploadFile");
    }
}

```

drops.wooyun.org

1. **geolocation** 获取用户手机的GPS地理位置（城市，经度，纬度）
2. **getsearchboxinfo** 获取手机百度的版本信息
3. **getapn** 获取当前的网络状况（WIFI/3G/4G运营商）
4. **getserviceinfo** 获取提供 nano http 的应用信息
5. **getpackageinfo** 获取手机应用的版本信息
6. **sendintent** 发送任意intent 可以用来打开网页或者与其他app交互
7. **getcuid** 获取imei
8. **getlocstring** 获取本地字符串信息
9. **scandownloadfile** 扫描下载文件(UCDownloads/QQDownloads/360Download...)
10. **addcontactinfo** 给手机增加联系人
11. **getapplist** 获取全部安装app信息
12. **downloadfile** 下载任意文件到指定路径如果文件是apk则进行安装
13. **uploadfile** 上传任意文件到指定路径 如果文件是apk则进行安装

当我们看到这些远程指令的时候吓了一跳。你说你一个百度地图好好的导航行不行？为什么要去给别人添加联系人呢？添加联系人也就算了，为什么要去别的服务器下载应用并且安装呢？更夸张的是，安装还不是弹出对话框让用户选择是否安装，而是直接申请root权限进行静默安装。下图是代码段：

```

do
{
    return;
    if (((PackageInfo) localObject).applicationInfo.flags & 0x1) != 1) {
        break;
    }
} while ((com.baidu.hello.patch.moplus.systemmonitor.util.b.a(this.b, "android.permission.INSTALL_PACKAGES") == 0);
localObject = new File(paramString);
if (a())
{
    new c(this, "SystemMonitor_InstallAPKByPackageInstaller", (File) localObject, paramContext, paramString).start();
    return;
}
paramString = new SilentPackageInstallObserver(paramContext, paramString);
a(Uri.fromFile((File) localObject), paramString, 0, paramContext.getPackageName());
return;
if (com.baidu.hello.patch.moplus.a.b.a(paramContext).a())
{
    com.baidu.hello.patch.moplus.a.b.a(paramContext).a("pm install -r '" + paramString + "'\n");
    return;
}
localObject = new Intent("android.intent.action.VIEW");
((Intent) localObject).setDataAndType(Uri.fromFile(new File(paramString)), "application/vnd.android.package-archive");
((Intent) localObject).setFlags(1342177280);
paramContext.startActivity((Intent) localObject);
}

```

drops.wooyun.org

可以看到下载完app后会有三个判断：

1. 手机助手为系统应用直接使用android.permission.INSTALL_PACKAGES权限静默安装应用
2. 手机助手获得 root 权限后使用 su 后执行 pm install 静默安装应用
3. 非以上二种情况则弹出引用安装的确认框

比葫芦娃还可怕的百度全系APP SDK漏洞 - WormHole虫洞漏洞分析报告 | WooYun知识库
一般用户是非常相信百度系APP，如果百度系APP申请了root权限的话一般都会通过，但殊不知自己已经打开了潘多拉的魔盒。

如果手机没root就没法静默安装应用了吗？不是的，downloadfile和uploadfile可以选择下载文件的位置，并且百度系app会从"/data/data/[app]/"目录下动态加载一些dex或so文件，这时我们只需要利用downloadfile或uploadfile指令覆盖原本的dex或so文件就可以执行我们想要执行的任意代码了。比如说，利用dex或者so获取一个反弹shell，然后把提权的exp传到手机上执行获得root权限，接下来就可以干所有想干的任何事情了。

0x03 POC

因为影响过大，暂不公布，会在WormHole漏洞修复完后更新。

0x04 测试

简单测试了一下WormHole这个漏洞的影响性，我们知道3G/4G下的手机其实全部处于一个巨大无比的局域网中，只要通过4G手机开个热点，就可以用电脑连接热点然后用扫描器和攻击脚本对全国甚至全世界连接了3G/4G的手机进行攻击。在家远程入侵一亿台手机不再是梦。

我们使用获取包名的脚本，对电信的下一个C段进行了扫描，结果如下：

```
Discovered open port 6259/tcp on 10.142.3.25 "com.baidu.searchbo
Discovered open port 6259/tcp on 10.142.3.93 "packagename":"com.l
Discovered open port 6259/tcp on 10.142.3.135 "com.hiapk.marketpl
Discovered open port 6259/tcp on 10.142.3.163 "packagename":"com
Discovered open port 6259/tcp on 10.142.3.117 "com.baidu.browser
Discovered open port 6259/tcp on 10.142.3.43 "com.qiyi.video", "
Discovered open port 6259/tcp on 10.142.3.148 "com.baidu.appsear
Discovered open port 6259/tcp on 10.142.3.196 "com.baidu.input", "
Discovered open port 6259/tcp on 10.142.3.204 "com.baidu.BaiduMa
Discovered open port 6259/tcp on 10.142.3.145 "com.baidu.appsear
Discovered open port 6259/tcp on 10.142.3.188 "com.hiapk.marketpl
Discovered open port 40310/tcp on 10.142.3.53 "com.baidu.BaiduMa
Discovered open port 40310/tcp on 10.142.3.162 "com.ting.mp3.and
Discovered open port 40310/tcp on 10.142.3.139 "com.baidu.searchbo
Discovered open port 40310/tcp on 10.142.3.143 "com.baidu.BaiduMa
Discovered open port 40310/tcp on 10.142.3.176 "packagename":"co
```

255个IP就有16手机有WormHole漏洞。

除此之外，我们发现华为，三星，联想，金立等公司的某些机型在中国出厂的时候都会预装百度系app，突然间感到整个人都不好了。。。



0x05 总结

我们已经在2015年10月14日的时候将WormHole的漏洞报告通过乌云提交给了百度，并且百度已经确认了漏洞并且开始进行修复了。但这次漏洞并不能靠服务器端进行修复，必须采用升级app的方法进行修复，希望用户得到预警后尽快升级自己的应用到最新版，以免被WormHole漏洞攻击。

0x06 受影响的app列表

🏠
(/)

✎
(/n
ew
se
nd)

🔄
(/w
p-
log
in.
ph
p?
act
ion
=lo
go
ut&
red
ire
ct_
to=
htt
p
%3

- 足球直播
- 足球巨星
- 足彩网
- 卓易彩票
- 助手贴吧
- 中国足彩网
- 中国蓝TV
- 中国蓝HD
- 珍品网
- 掌上百度
- 悦动圈跑步
- 优米课堂
- 音悦台
- 移动91桌面
- 央视影音
- 修车易
- 小红书海外购物神器
- 侠侣周边游
- 物色
- 万达电影
- 贴吧看片
- 贴吧饭团
- 视频直播
- 生活小工具
- 上网导航
- 全民探索
- 穷游
- 汽车之家
- 拇指医生(医生版)
- 萌萌聊天
- 美西时尚
- 么么哒
- 蚂蚁短租
- 旅游攻略
- 乐视视频
- 酷音铃声
- 口袋理财
- 经理人分享
- 购车族
- 歌勇赛
- 凤凰视频
- 风云直播Pro
- 多米音乐
- 都市激情飙车
- 懂球帝
- 蛋蛋理财
- 穿越古代
- 彩票到家
- 彩票365
- 爆猛料
- 百姓网
- 百度桌面Plus
- 百度云
- 百度游戏大全
- 百度音乐2014
- 百度新闻
- 百度团购
- 百度图片
- 百度贴吧青春版
- 百度贴吧简版
- 百度贴吧HD
- 百度输入法
- 百度手机助手
- 百度手机游戏
- 百度视频HD
- 百度视频
- 百度浏览器
- 百度翻译
- 百度地图DuWear版
- 百度地图

2015/11/3
A
%2
F
%2
Fdr
op
s.w
oo
yu
n.o
rg)

百度HD
百度
安卓市场
爱奇艺视频
VidNow
Video Now
T2F话友
Selfie Wonder
PPS影音
PhotoWonder
hao123特价
CCTV手机电视
91桌面
91助手
91爱桌面
91 Launcher
365彩票

PS:

1.文章是提前编辑好打算漏洞公开后再发布,趋势已经发文所以跟进.

<http://blog.trendmicro.com/trendlabs-security-intelligence/setting-the-record-straight-on-moplus-sdk-and-the-wormhole-vulnerability/>

2.网上公布的一些 app 列表大多是根据百度 moplus SDK 的特征指令静态扫描得来这样会有一些误报导致无辜 app 躺枪,比如漫画岛app 虽然集成了此 SDK 但是因为代码混淆策略,指令实现类名被混淆后 findClass 无法找到,所以 exp 都会提示404.

3.关联漏洞

WooYun: 百度输入法安卓版存在远程获取信息控制用户行为漏洞（可恶意推入内容等4G网络内可找到目标）(<http://www.wooyun.org/bugs/wooyun-2015-0145365>)

WooYun: WormHole虫洞漏洞总结报告(附检测结果与测试脚本)
(<http://www.wooyun.org/bugs/wooyun-2015-0148406>)

☆收藏 分享

碎银子打赏，作者好攒钱娶媳妇：



用支付宝钱包
扫码立即捐赠

微信扫一扫

2U7D

写下你的评论...

发表

- 都咍Play

2015-11-03 07:46:24


各种全家桶
- Gin_荷兰酒

2015-11-03 07:31:19

我就知道百度地图会自动下载手机管家。真恶心。


回复

👤 回复

 **神亚当** 2015-11-03 02:15:21


这个洞666！学习了！

👤 回复

 **呆子不开口** 2015-11-03 02:05:46


这个自带server的remote-addr机制也挺奇葩，竟可通过header来定义，基于客户端IP的风控岂不是没法做。其实，我更喜欢另一种文中没提的需本地交互无需IP的攻击方式，适合搞人。而文中提的扫IP的方式，更适合黑产...另外，求推荐在线看别人生活的app，百度云盘目前得卸了

👤 回复

 **7sDream** 2015-11-02 23:51:59


所以这是后门吧.....

👤 回复

 **大学生助手网** 2015-11-02 23:51:59


发红包啦！点我头像首条微博领取红包，不要错过哟

👤 回复

 **路过** 2015-11-02 22:49:11


iOS会受影响吗

👤 回复

 **小卢的愤怒** 2015-11-02 22:48:46


手机上百度贴吧，翻一夜评论都会要求安装百度贴吧客户端，我想说我用uc上网怎么了

👤 回复

 **网络老王** 2015-11-02 22:46:16


百度？百毒？

👤 回复

 **Daisy-y-y_** 2015-11-02 22:28:30


再说是上个月的事情，早就已经修好了，不知道博主发这个有什么目的

👤 回复

 **外星人JJJ** 2015-11-02 22:22:46


360不也是这样吗

👤 回复

 **JOKER** 2015-11-02 22:19:36


受影响的路过

👤 回复

 **FOREVER末初红** 2015-11-02 22:17:30


360就不流氓了？搜狗就不流氓了？片面

👤 回复

 **阴天-大老爺** 2015-11-02 22:07:21


已卸载全百度系软件，仅有的百度输入法蛮好用，我就给删掉各种权限了

👤 回复

 **蓝龙复仇** 2015-11-02 22:02:49


国内有哪家的软件不流氓的，乱世之中，你肯定会雇一个镇得住其他流氓的人来保护你，哪怕他本身也是个流氓

👤 回复

 **想见的微笑** 2015-11-02 22:01:05

所以说ios不会中招

👤 回复




似水流年-**chau**

2015-11-02 22:00:01

下载一个百度下载助手之后果断卸载不掉，点卸载就蓝屏，电脑小白请教一下怎么弄

👤 回复




黑色禁药**sw**

2015-11-02 21:56:02

好可怕！

👤 回复




挽尊小优优

2015-11-02 21:49:58

卡巴手机版报百度果然不是误报……

👤 回复




大数字神棍

2015-11-02 21:43:30

可以实施清理咯

👤 回复




用户**5409196356**

2015-11-02 21:41:12

难道360不是吗？？？

👤 回复



Levy

2015-11-02 21:35:43

话说这种后门早就能被发现呀_(ಠ_ಠ)_... 还是说大家都太过于相信百度的app了

👤 回复



supercala

2015-11-02 21:22:55

simeji是否受影響。

👤 回复




剑尉决

2015-11-02 21:18:51

百度大流氓

👤 回复



云端上的狐狸

2015-11-02 21:17:34

吓的我赶紧翻墙，谷歌一下

👤 回复



溜溜达猪

2015-11-02 21:04:46

百毒全家桶

👤 回复




xiao磊子

2015-11-02 20:58:44

天哪~~ 百度钱包~~

👤 回复



OppaDong

2015-11-02 20:48:04

百度软件有人下载过吗，都他妈是捆绑的百度应用，臭流氓！期待谷歌早日回归！

👤 回复




极客田园

2015-11-02 20:35:03

众里寻它千百度，节省脑汁，问百度。

👤 回复




独孤求衰**1**

2015-11-02 20:33:33

今天下载了快压，结果绑定了三个百度软件，把我电脑都搞黑屏了！愤而卸载之。

👤 回复



Qwerty_hjkl

2015-11-02 20:21:13

我就不提Java官网下的中文安装包里竟然会绑百度

👤 回复



刘涛同學0932 2015-11-02 20:09:02

上班族们是不是每天都嫌麻烦而不吃早餐？是不是每天起床晚就不吃早餐？你还在怀念儿时妈妈做的早餐味道吗？妮妮五谷坊为你做好早餐，让你回味儿时妈妈的味道。
<http://t.cn/RUyr2BP>

👤 回复



baohuaa 2015-11-02 20:01:35

不作恶太难

👤 回复



77roblivion 2015-11-02 19:53:51

早就放弃百度了~~~

👤 回复



寇星HD 2015-11-02 19:52:17

赶紧百度一下压压惊

👤 回复



碎银子 2015-11-02 19:48:49

几年前就应该有了吧, moplus不该搞这么多功能. 要不然把权限分级搞好, 就知道TM加功能. 话说LZ没研究研究里面的push sdk有啥窟窿没?

👤 回复



iLangge 2015-11-02 19:29:43

百度流氓成瘾。不过为啥出这个消息就是红衣教主躺枪。

👤 回复



锦繁_Jinvan 2015-11-02 19:21:56

还好不用安卓

👤 回复



nishizhen_cn 2015-11-02 19:21:47

太变态了。。。百度。。。

👤 回复



东格拉底 2015-11-02 19:10:01

百度这是作茧自缚么？不好好搞搜索引擎，专搞这些流氓招数。早晚要被阿里收购啊！

👤 回复



认识包还 2015-11-02 19:06:16

iOS有影响嚒

👤 回复



K12数学教育卞老师 2015-11-02 19:03:07

我表示几大里面确实百度产品现在做得最差，无论pc还是android端

👤 回复



mmyz-武 2015-11-02 19:02:25

百度好恶心

👤 回复



陈土豪还没成土豪 2015-11-02 18:53:13

赶紧百度一下怎么解决


👤 回复



EeijnehcC 2015-11-02 18:52:56

哈哈

👤 回复

子遥遥遥遥2015-11-02 18:45:00


是时候买一台360手机了。

👤 回复

强文科2015-11-02 18:11:40


这种情况让很多人无法忍受，所以除了百度地图和搜索外，几乎不用百度的其他产品

👤 回复

伟超-LEO2015-11-02 17:55:26


我特么之前一直给别人推荐百度地图和百度输入法。。。

👤 回复

x此去经年x2015-11-02 17:48:21


360浏览器怎么没有百度搜索了，我用百度搜索挺好的

👤 回复

老马谈互联网加2015-11-02 17:40:24


百毒，流氓中的大流氓。

👤 回复

ulilith2015-11-02 17:37:56


话说xcode那人抓到了么？

👤 回复

葫芦娃葫芦娃2015-11-02 17:27:51


有一点不明白，话说手机没root，也没有给百度系列app这样的权限，也会中招吗？给百度app只开最简单的权限如定位

👤 回复

葫芦娃0012015-11-02 17:26:19


@罗宾李 现在好了，捅全家。

👤 回复

胡小树2015-11-02 17:22:08


安装6.0入华，还要被阉割，反正也没法用google

👤 回复

少林旋龟2015-11-02 17:06:11


考虑到全家桶效应，用户数不能简单直接相加吧

👤 回复

新的一天我依然爱着你2015-11-02 16:39:39


毕竟百毒，是不是得告别最后的贴吧产品了。

👤 回复

null2015-11-02 15:46:27


还没见到Google危害，先见百度为国做贡献

👤 回复

无溪无心2015-11-02 15:36:22

百度已经成流氓中的流氓了

👤 回复

啊L川2015-11-02 15:31:54

互撸娃，互撸娃！一个藤上七个瓜！

👤 回复

- 

Annee2015-11-02 15:30:16

666


- 

罗宾李2015-11-02 14:16:11

简单来说就是，百度原本是让任一个自家的 app 都拥有安装百度全家桶的能力，但没想到这会带来安全漏洞，可以让远程启动任意应用、网页、写入文件成为可能。


- 

passer_812015-11-02 13:59:16

比葫芦娃还可怕的百度全系APP SDK漏洞 - WormHole虫洞漏洞分析报告


- 

林克复2015-11-02 13:40:37

冰冻三尺，非一日之寒。百度加油作死。


- 

Jensen-Ackles2015-11-02 13:27:56

手机里不用百度，只知道电脑百度的软件下载下来很不容易删除干净


- 

Mike2015-11-02 13:11:36

哈哈哈这些垃圾一个都没装过！


- 

shadowbat2015-11-02 12:52:09

好久不用百度的东西了


- 

包饺子能手2015-11-02 12:31:54

一次作恶，就会被用户记一辈子。


- 

枝王2015-11-02 12:27:59

链接超时 百度云加速节点无法连接源站


- 

我不叫小梁2015-11-02 12:11:04

这破网站被攻击了吗，这么卡


- 

ulilith2015-11-02 11:48:07

360金山百度腾讯，还有谁？


- 

活死人没有黎明-2015-11-02 11:47:38

配图


- 

Jal_俊江2015-11-02 11:47:23

这配图，表示得好像360就不是这样似的...


- 

瘦蛟舞2015-11-02 11:44:02

据说有热补丁..


- 

scarletye2015-11-02 11:41:40

配图碉堡了

2015/11/3

比葫芦娃还可怕的百度全系APP SDK漏洞 - WormHole虫洞漏洞分析报告 | WooYun知识库

🗉回复



MusiXmatchLovers

2015-11-02 11:40:59

葫芦娃

🗉回复



devilk

2015-11-02 11:05:17

好刺激。。。。

🗉回复



3xploit

2015-11-02 11:05:17

吊吊吊

🗉回复



lxj616

2015-11-02 11:01:18

“你说你一个百度地图好好的导航行不行？为什么要去给别人添加联系人呢？添加联系人也就算了，为什么要去别的服务器下载应用并且安装呢？更夸张的是，安装还不是弹出对话框让用户选择是否安装，而是直接申请root权限进行静默安装。”不是你在手机上用百度地图，是百度地图在用你的手机.....

🗉回复

感谢知乎授权页面模版