360 手机精灵、豌豆荚、腾讯应用助手
漏洞分析报告

报告摘要

近日，360 手机精灵、豌豆荚、腾讯应用助手等手机辅助管理软件被爆存在安全隐患，会导致用户手机内存、存储卡的数据（照片、短信、聊天记录、电话录音、视频以及其他文档）等个人数据不经允许被第三方恶意访问、上传、下载、或篡改、删除。

运行 Android 平台的智能手机在全球的市场份额约 22%，中国又是全球智能手机拥有量最多的国家。据分析，截止 2011 年第三季度，中国网民拥有的 Android 手机总量约 2500 万台，超过 iphone 手机拥有量。因此，360 手机精灵等 Android 手机辅助管理软件的安全漏洞可能影响数千万 Android 手机用户。

金山毒霸安全中心对上述软件存在信息泄露漏洞的情况进行了详细技术分析和验证，详细如下：

【 三款手机辅助管理软件存在信息泄露风险的简单分析】

	360 手机精灵	豌豆荚	腾讯应用助手
使用固定用户名密码	是，不安全	是，不安全	安全
使用固定端口号	是，不安全	是，不安全	安全
安装过程是否有明确提示	PC 端模糊提示，手机端无提示	均有提示	均有提示
实现方式安全性	FTP（不安全）	FTP（不安全）	Socket（较安全）
用户密码容易得到程度	容易	容易	困难
解决方案是否完善	存在潜在问题	存在功能缺失	较完善
通讯是否有动态验证	没有（不安全）	没有（不安全）	有（安全）

可以看到：

360 手机精灵：360 安全卫士的覆盖面和其不经明示，连接手机即安装 360 手机精灵的特点，360 手机精灵的漏洞影响的用户面最大。

豌豆荚：该软件通过 Wifi 下去掉文件管理器功能的方式来处理该问题，造成产品功能的缺失，同时该软件的验证码机制由于在同一机器，同一无线环境下不会变化，因此仍存在一定风险。

腾讯应用助手：该软件通过强度较高的 socket 的点对点的通信方式，只有在机器本身中木马，或者 Hub 被抓包的情况下，才存在安全风险，该种情况大部分软件的安全性都会受到波及，因此影响面最小。

目前，三款软件均已经修复原有产品漏洞，金山毒霸安全中心对其修复方案进行技术分析，详细如下：

【三款 Android 手机辅助管理软件存在信息泄露漏洞的评估及解决方案】

产品名称	威胁等级	漏洞特点	解决方案
360 手机精灵	 严重	1.360 手机精灵用户名和密码极容易获得； 2.ftp 服务长驻，开机自启动； 3.很容易被利用； 4.手机连接电脑充电即被无提示安装； 5.通过 360 安全卫士捆绑推广。	限制为本机 IP 才能访问，ftp 服务仍然存在，用户名密码可轻松获取，仍然可能被恶意程序和网站利用。
豌豆荚	 中等	1.开机不会自动启动，电脑运行豌豆荚客户端，同时插上手机数据线时，豌豆荚才进行启动； 2.密码需要通过反编译得到，需要更高的专业知识，不容易被普通用户掌握。	在 Wifi 环境下，不再提供文件管理功能，漏洞风险得到避免；
QQ 应用助手	 轻度	1.QQ 使用 socket 连接方式，外网缺少对此类利用的工具； 2.动态验证码机制，比以上两款软件都更加安全。	只有输入动态验证码才能进行访问，相对以上两者都更加安全和完善。

结论：360 手机精灵的解决方案依然遗留了较大的安全风险，豌豆荚和 QQ 应用助手的解决方案技术完善性更佳。

金山毒霸安全中心提示软件企业，功能的便利性不能以牺牲用户数据安全为代价，希望各手机软件管理厂商能够积极协商制定技术规范，进行技术交流和指导，促进行业发展。

详细分析

一、对 360 手机精灵的分析

1. 情况概述

对 360 手机精灵样本进行了深入分析，主要结论包括：

- 在涉及公司主站以及第三方下载站发现存在该问题样本；
- 国内用户手机中间存在该样本；
- 样本会开启一个 FTP 服务；
- 样本使用了固定的用户名和密码；
- 样本会使用 360 安全卫士作为主安装渠道，在没有明示用户的情况下，连接手机充电，即会安装到 Android 手机上；
- 在 Wifi 模式下，没有对访问来源进行限制；
- FTP 密码为明文保存易被恶意利用

2. 影响版本

360 手机精灵 1.31 之前版本的用户，包括 1.30、1.20 等版本

3. 漏洞现象

在安装 360 安全卫士的机器上，插上数据线会弹出管理手机对话框

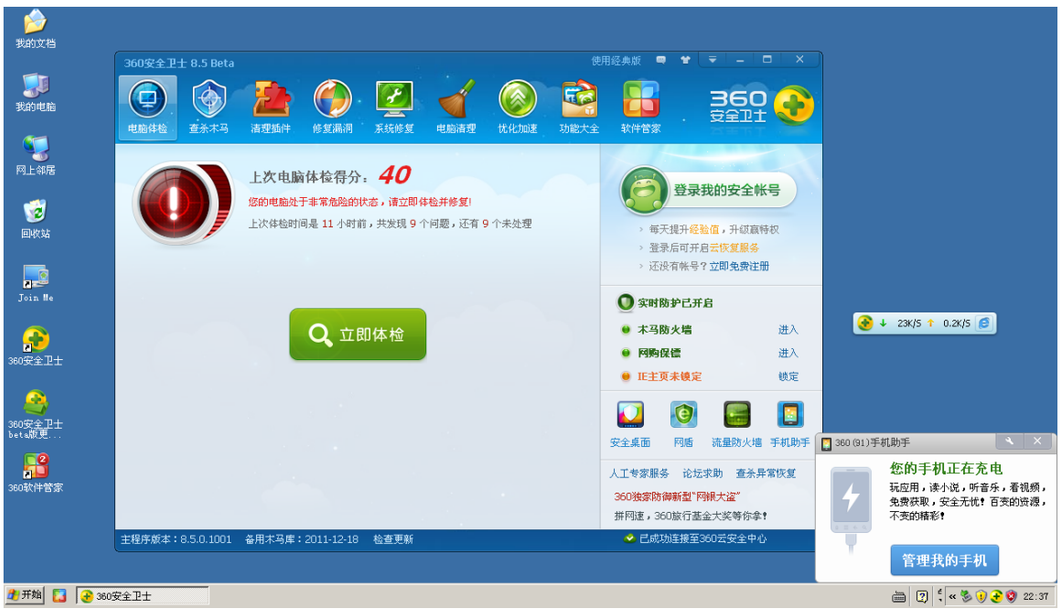

图 2 手机连接电脑充电时，360 弹窗提示管理手机

点击管理我的手机按钮。会提示正在连接手机

图 3 360 手机助手正在连接 Android 手机

这时会不经用户确认自动安装 360 手机精灵

图 4 PC 端提示安装 360 手机精灵，手机端不会有任何提示

静默安装后，会出现 360 手机助手界面

图 5 360 手机助手主界面

这时候查看手机的设置|应用程序中，就会发现 360 手机精灵程序已经被安装

图 6 Android 手机中 360 手机精灵被安装

360 手机精灵会在后台运行，点击运行可以看到如下界面：

图 7 手动运行 360 手机精灵的界面

此时如果开着 Wifi 网络，则其他 Wifi 用户可以通过 360 手机精灵的漏洞，远程登录 FTP 服务连接到这部手机上。

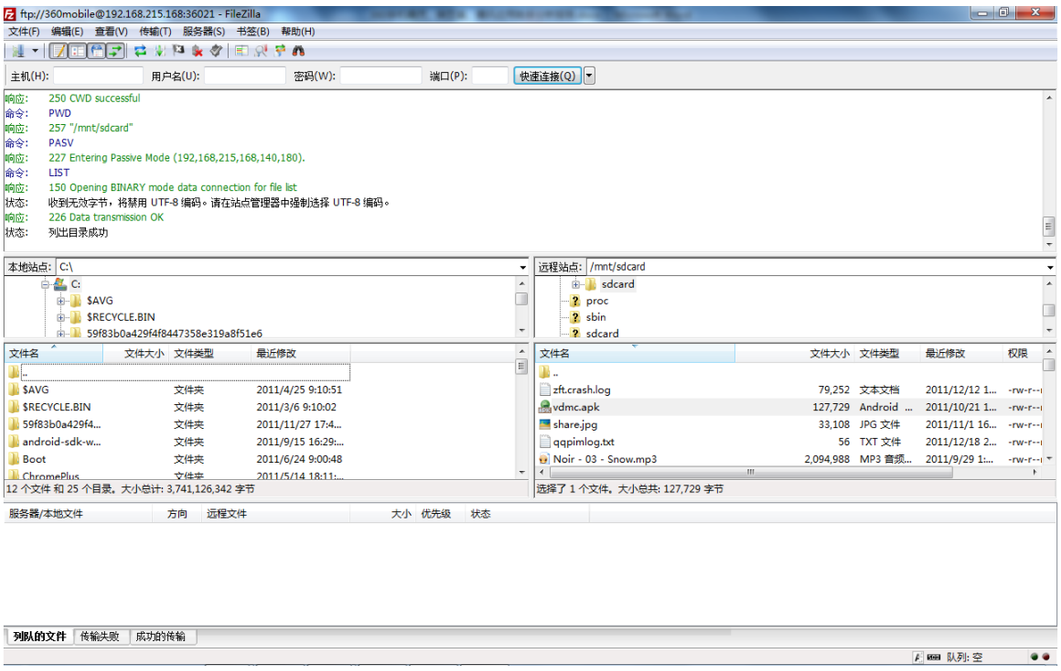

图 8 其他接入 wifi 的电脑可访问安装了 360 手机精灵的 Android 手机

此时可以对手机中的内容进行浏览、下载、删除操作。

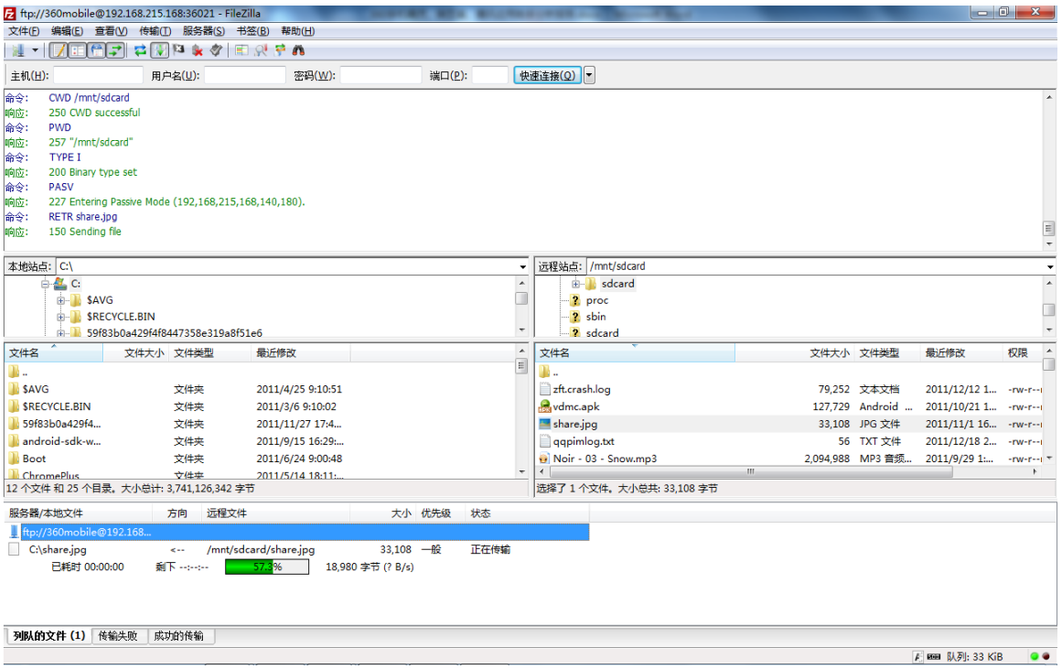

图 9　安装了 360 手机精灵的 Android 手机中存储卡数据正在被下载和进行删除操作

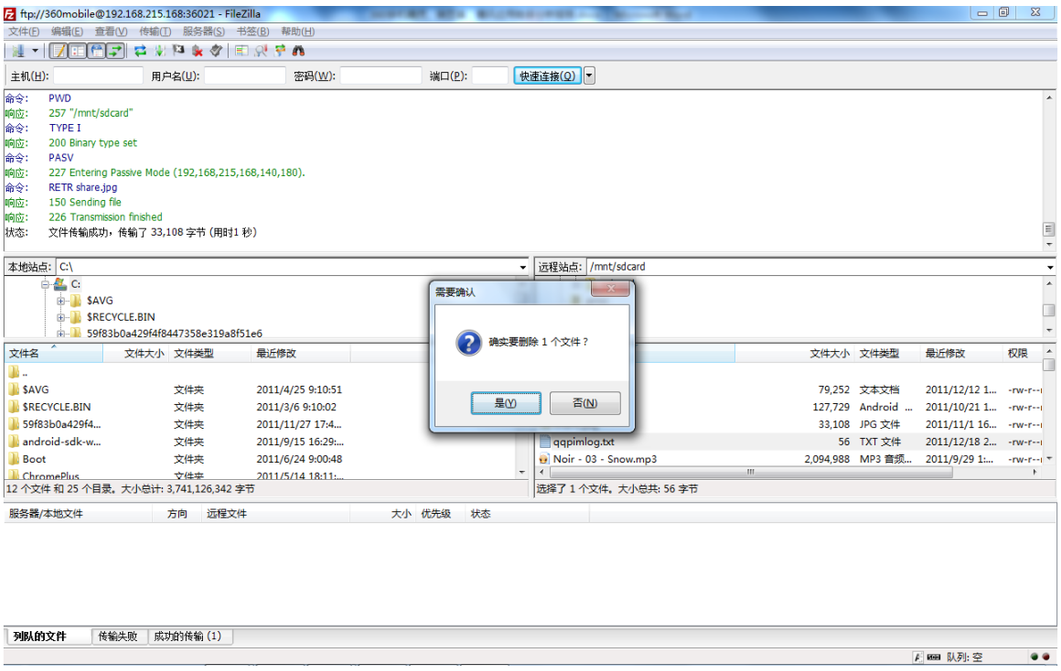

图 10 FTP 客户端远程删除安装了 360 手机精灵的 Android 手机存储卡数据确认后就删除了

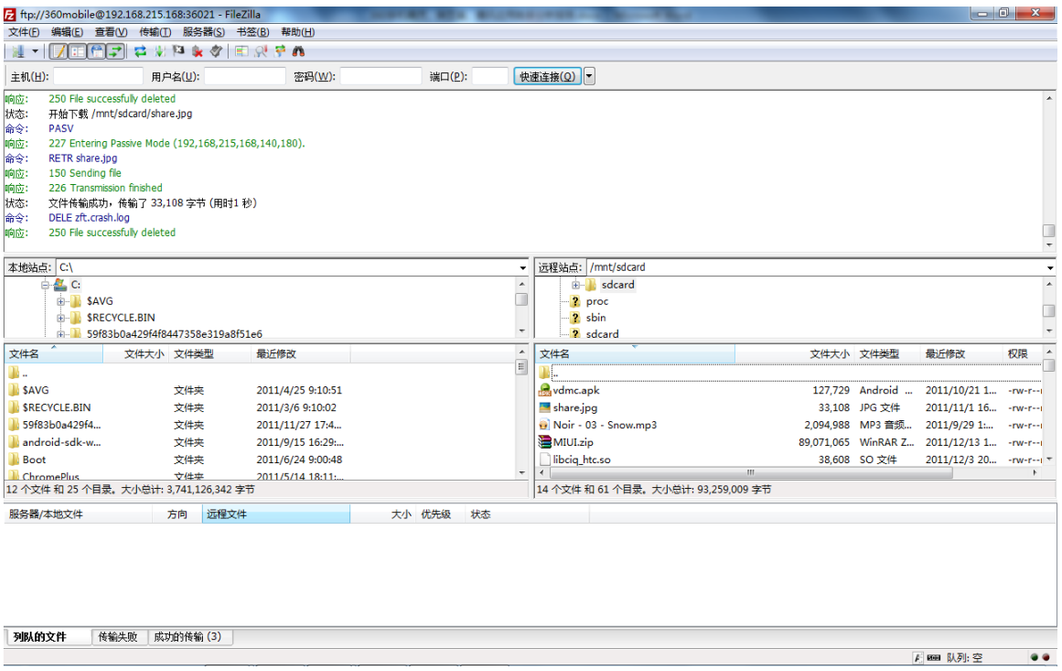

图 11 安装了 360 手机精灵的 Android 手机存储卡数据被远程删除

4. 技术分析

程序版本：

com.qihoo360.daemon 1.3.0

漏洞描述：

360 手机精灵提供文件管理功能，这个功能是 360 手机精灵实现的一个 ftp 服务来管理文件，ftp 的密码明文保存在程序的配置文件中，登录 ftp 时由于没有限制客户端，导致
在同一 AP（无线网热点） 下的其他用户可以浏览、上传、下载、删除安装有 360 手机精灵的手机的 sdcard 里面的内容，手机内存目录可浏览、下载。

具体分析如下：

从 AndroidManifest.xml 看到，360 手机精灵开机自启动，然后后台有一个守护后台服务，监听来至 pc 端的 ftp 连接

```
<service
    android:name="com.qihoo360.mobilesafe.pcdaemon.service.DaemonService"
    android:exported="true"
    >
</service>

<uses-permission
    android:name="android.permission.RECEIVE_BOOT_COMPLETED"
    >
</uses-permission>
```

在主程序里面实现了一个 ftp 服务器

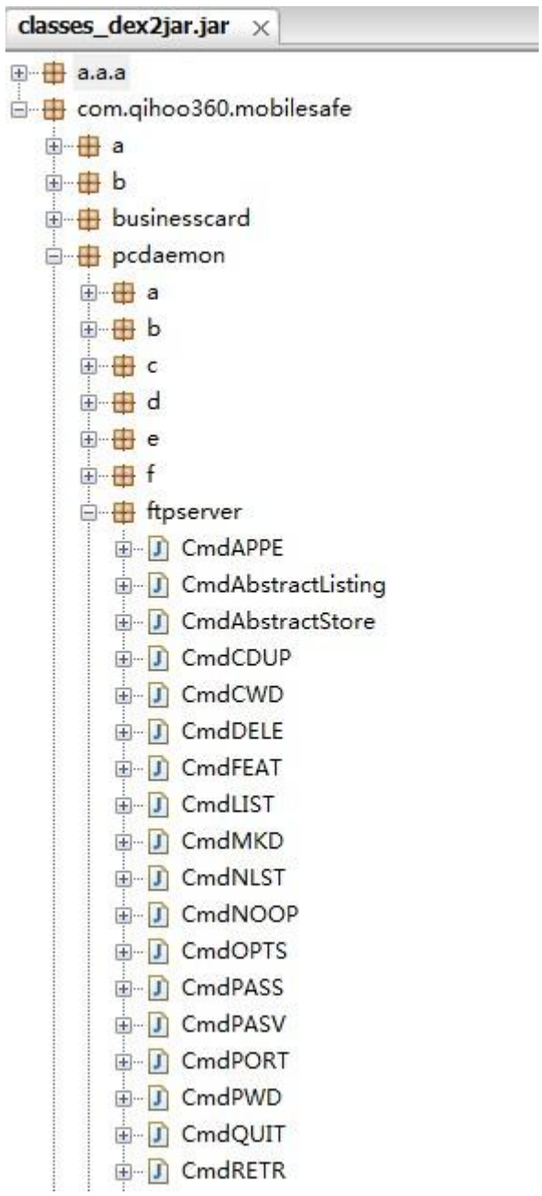

图 12 360 手机精灵内置的 Ftp 服务

其中有 DELE　STOR，列举文件等常用 ftp 命令，在后台 DaemonService 服务中，我们会看到开启了 ftp 监听服务，等待 pc 客户端连接

```
try
{
  this.h = new com.qihoo360.mobilesafe.pcdaemon.ftpserver.e(this);
  if (com.qihoo360.mobilesafe.a.a.a);
  for (int i = 2; ; i = 6)
```

图 13 360 手机精灵 FTP 服务属性

由于 360 手机精灵会使用 SharedPreferences 把用户和密码明文存在本程序目录中

图 14 360 手机精灵的用户名、口令以明文方式保存

知道了用户名和密码，端口和 ftp 协议，我们可以开一个扫描器扫描局域网安装了 360 手机精灵的 Android 手机。

ftp 登陆没有限制，然后开机后台服务自启动，导致在 wifi 环境下，随意登陆 ftp 服务器,相当于 360 把你的手机提供给别人访问了。这样只要你安装了 360 手机精灵，在公用 wifi 环境下，就能访问你 sdcard 里面的东西了。许多程序喜欢备份通讯录，短信存在 sdcard 中，然而又没有加密（或者加密的强度很差，非常容易破解），这导致黑客直接存取你的信息。

解决方案

新版本中，在 Wifi 环境下只允许本机 IP 地址进行 FTP 登陆。

```
new-instance v2, Ljava/net/InetSocketAddress;

#v2=(UninitRef);
const-string v3, "127.0.0.1"

sget v4, Lcom/qihoo360/mobilesafe/pcdaemon/ftpserver/e;->i:

#v4=(Integer);
invoke-direct {v2, v3, v4}, Ljava/net/InetSocketAddress;-><
```

图 15 新版 360 手机精灵的修改

但尽管做了 IP 过滤限制，该方案依然存在被恶意程序或者网站利用的潜在风险；

二、对豌豆荚的分析

1. 情况概述：

对豌豆荚进行了深入分析，主要结论包括：

- 在涉及公司主站以及第三方下载站发现存在该问题样本；
- 国内用户手机中间存在该样本；
- 样本会开启一个 FTP 服务；
- 样本使用了固定的用户名和密码；
- 在 Wifi 模式下，没有对访问来源进行限制；

2. 漏洞现象

豌豆荚为了实现文件管理功能，使用了 FTP 服务，该服务使用了固定的用户名和密码，且因为该软件会自动启动并后台运行，在手机开启 Wifi 的情况下，同一无线路由器 AP 中，安装豌豆荚的用户均会受到威胁。

豌豆荚主界面

图 16 豌豆荚管理手机的主界面

在豌豆荚启动的情况下，此时如果开着 Wifi 网络，其他用户可以通过 FTP 服务连接到这部手机上

图 17 豌豆荚启动 Wifi 方式连接到 PC

此时可以连接到这部手机

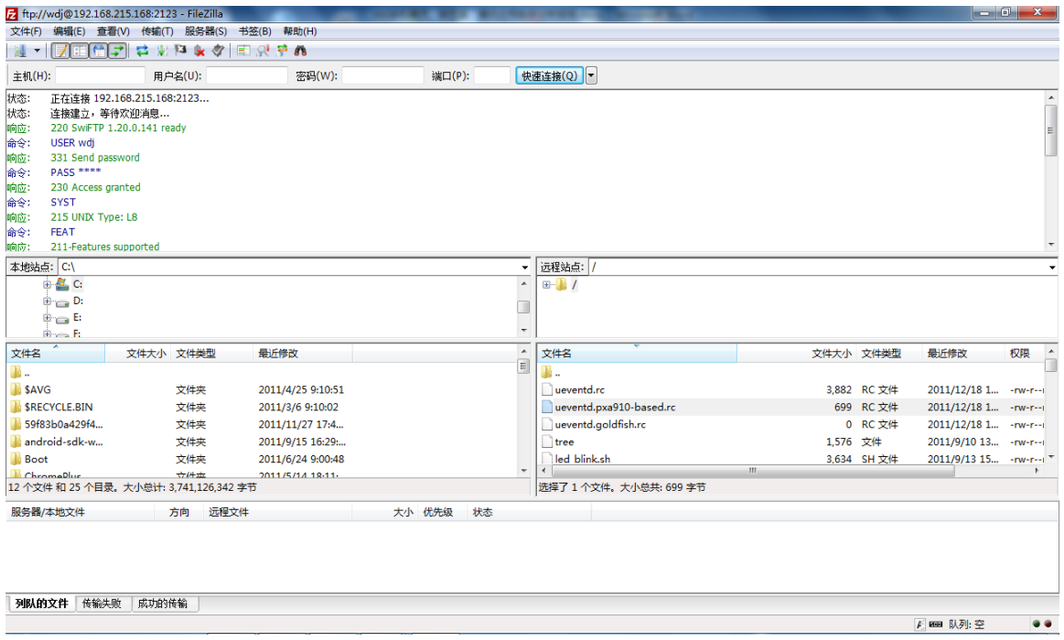

图 18 使用 FTP 客户端连接安装了豌豆荚的 Android 手机

同时对手机中的内容进行下载

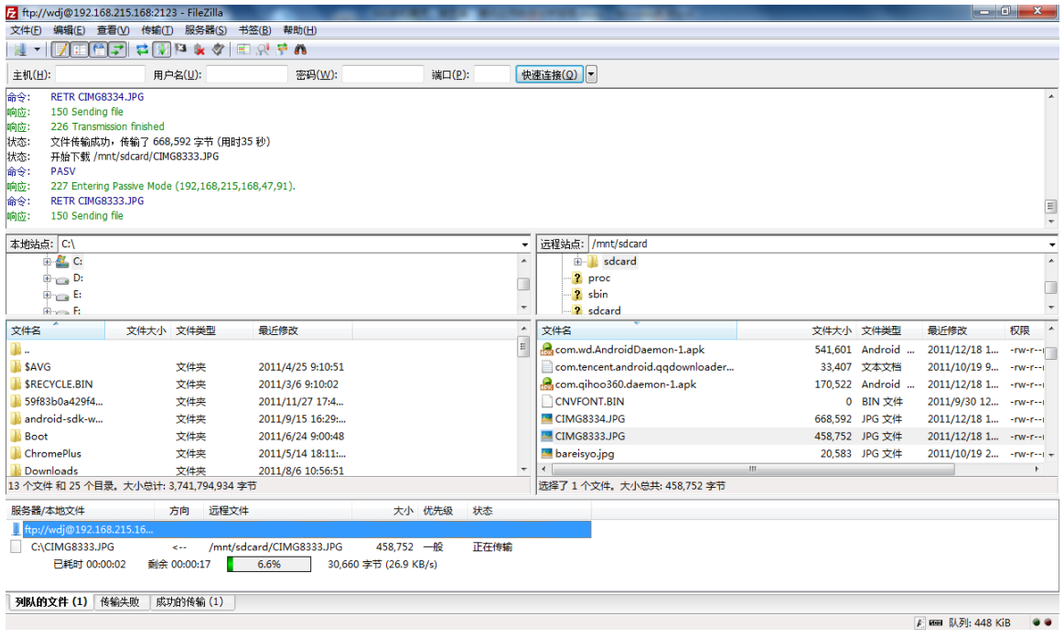

图 19 使用 FTP 客户端软件下载安装了豌豆荚的 Android 手机数据

和进行删除操作

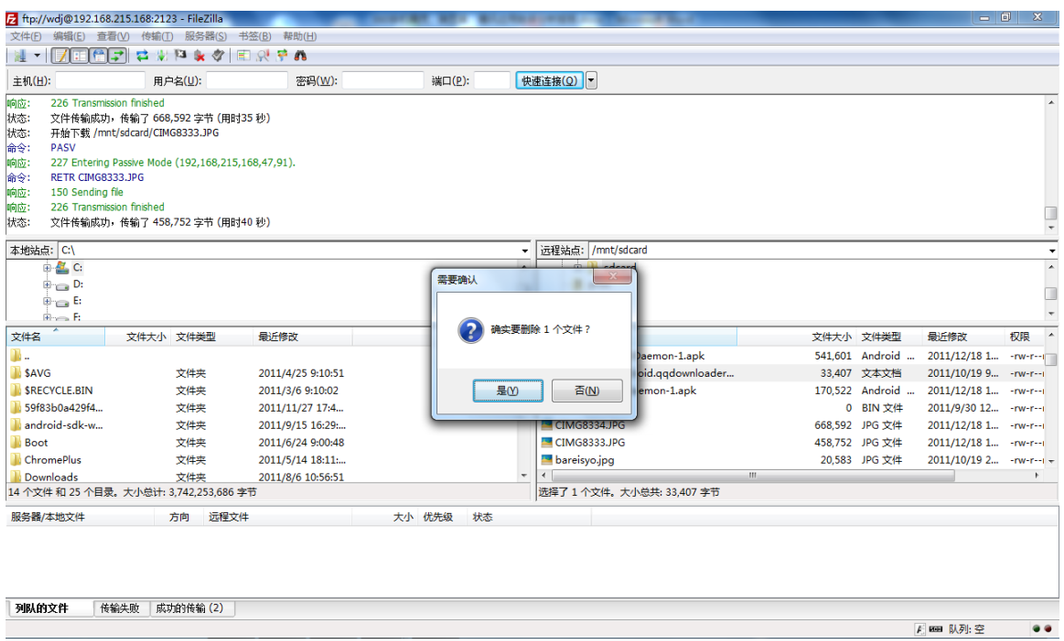

图 20 使用 FTP 客户端软件删除安装了豌豆荚的 Android 手机数据

确认后就删除了

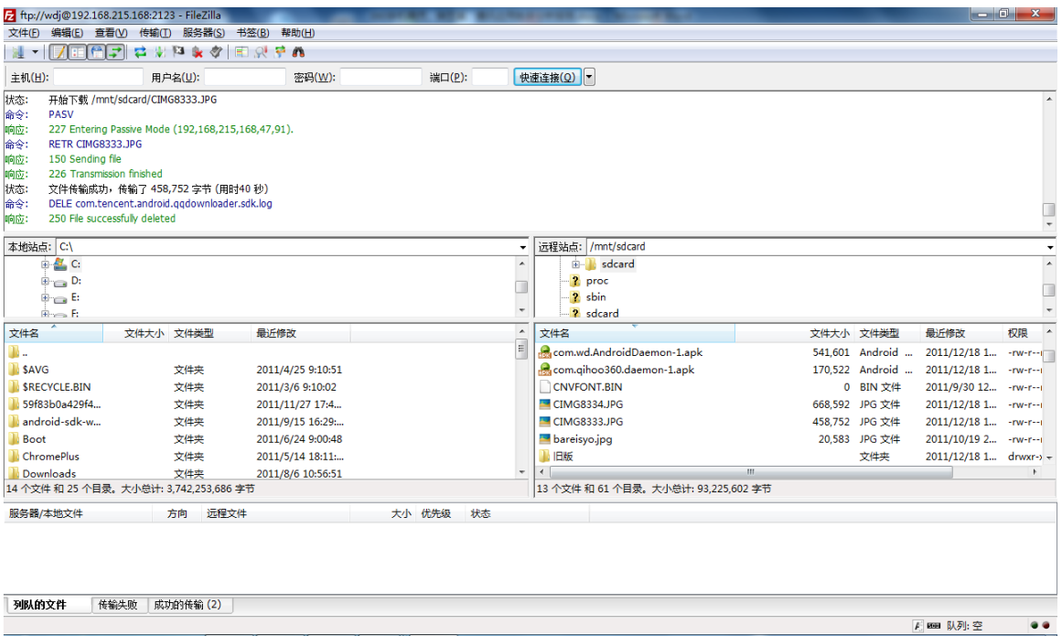

图 20 删除后的结果展示

3. 技术分析

漏洞版本：

com.wd.AndroidDaemon 1.8

漏洞描述：

豌豆荚使用 ftp 服务，用户名和密码直接写在程序中，登录 ftp 时由于没有限制客户端，导致在同一 AP（无线接入热点）下的其他用户可以浏览、上传、下载、删除安装有豌豆荚手机精灵的手机的 sdcard 里面的内容。

具体分析如下:

从 AndroidManifest.xml 看到，豌豆荚 android 端同样使用 ftp 提供 File 管理功能

```
<service
    android:name="com.wd.core.server.ftp.WandouFileService">
</service>
```

在反编译的类 WandouFileService.class 里面我们能看到

```
String str1 = a.f;
String str2 = a.g;
if ((str1 == null) || (str2 == null))
  Log.e("[FTP]", "Username or password is invalid");
```

图 21 分析豌豆荚手机端（1）

密码和用户名就是 a.f 和 a.g 中，在混淆的 a 类中，可以看到默认的用户和密码

```
protected static String f = "[redacted]";
protected static String g = "[redacted]";
```

图 22 分析豌豆荚手机端（2）

(豌豆荚的密码需要反编译才能获得，相对于 360 手机精灵较难被普通用户掌握)

解决方案：

豌豆荚取消了通过 FTP 文件管理的功能，在 Wifi 的 tcp 连接中让用户输入生成的验证码，但是这个 tcp 链接依然不安全，这个验证对于同一台手机来说会不变，依然有问题，可以用 tcp 连接来访问联系人以及短信。

影响版本

安装豌豆荚 1.1.24.1.1396 之前版本的用户，包括豌豆荚 1.23.1 等版本

修补方案分析

豌豆荚在 Wifi 环境下，取消了 SD 卡文件管理功能，造成产品功能缺失

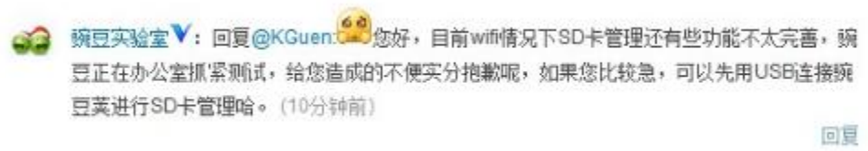

图 23 豌豆荚官方就修补方案发表微博

此外豌豆荚使用 TCP 链接，让用户输入生成的验证码，这个验证码在同一无线网络环境下的同一台手机来说是会不改变，在破解验证码算法后，存在通过该方式读取联系人和短信信息的威胁。

三、对腾讯应用助手的分析

1. 情况概述：

金山对腾讯应用助手进行了深入分析，主要结论包括：

- 动态验证进行验证；
- 使用 socket 连接进行连接，相对较为难被利用；

2. 技术分析

漏洞版本：

腾讯应用助手(安卓软件管理)v1.0 Beta3

漏洞描述：

腾讯应用助手使用 socket 连接，在 socket 连接中，由于没有限制客户端，导致在同一 AP 下的其他用户可以随意存取安装有 QQ 应用助手的手机的 sdcard 里面的内容，虽然这种连接理论上能劫持，但是要由于需要验证码，只有仔细分析算法后，写出验证码算法后才能连接，安全的强度不够。

技术分析

从 AndroidManifest.xml 看到，腾讯应用助手开机自启动，然后后台有一个守护后台服务，监听来至 pc 端的 socket 连接,如下：

```
<service
        android:name="com.qq.AppService.AppService" >
    </service>

<uses-permission
    android:name="android.permission.RECEIVE_BOOT_COMPLETED"
    >
</uses-permission>
```

在 com.qq.AppService.AppService，根据连接方式选择 wifi 连接还是 usb 连接

```
public void run()
{
  byte[] arrayOfByte1 = new byte[''];
  while (a)
  {
    DatagramPacket localDatagramPacket1 = new DatagramPacket(arrayOfByte1, 128);
    byte[] arrayOfByte2;
```

图 24 分析 QQ 手机助手

图 25 QQ 应用助手手机端启用 Wifi 连接

修补方案分析

在腾讯应用助手(安卓软件管理)v1.0 Beta4 版的更新日志中可以看到：

> 应用助手 for Android 1.0 Beta4 Fix2011-12-15
>
> 1. 修改 USB 连接流程，增加应用助手手机端安装提示
> 2. 新增 Wifi 连接确认,保证您的手机连接更加安全
> 3. wifi 连接时手机端增加 PC 连接的状态显示

在 Wifi 联网时，手机端有需要用户确认提示对话框，安全性得到很大提高。