南明离火
移动应用检测平台

ANDROID 静态分析报告

华润电力 • v1.2.3

分析日期: 2024-05-09 09:20:03

应用概览

文件名称:	PMS二期v1.2.4.apk
文件大小:	4.22MB
应用名称:	华润电力
软件包名:	com.pm360.superepip.hrdl
主活动:	com.pm360.superepip.ui.activity.WelcomeActivity
版本号:	1.2.3
最小SDK:	16
目标SDK:	23
加固信息:	未加壳
应用程序安全分数:	21/100 (重大风险)
跟踪器检测:	2/432
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	cad684e77a7ed4d9f34cd67128f7a0db
SHA1:	442da6eeb7873cd2fe6b2b6940b4a2aa1dbcb2cc
SHA256:	46722ba6bbab52840a54a5a0a31c3e097aedfe4ee6a920828feb96954b21544c

分析结果严重性分布

高危	中危	信息	安全	关注
23	17	1	0	7

四大组件导出状态统计

Activity组件：58个，其中export的有：1个
Service组件：7个，其中export的有：3个
Receiver组件：6个，其中export的有：4个
Provider组件：0个，其中export的有：0个

应用签名证书信息

二进制文件已签名
v1 签名: True

v2 签名: True
v3 签名: False
v4 签名: False
主题: C=cn, ST=jiangsu, L=nanjing, O=PM360, OU=PM360, CN=PM360
签名算法: rsassa_pkcs1v15
有效期自: 2016-06-29 02:39:26+00:00
有效期至: 2046-06-22 02:39:26+00:00
发行人: C=cn, ST=jiangsu, L=nanjing, O=PM360, OU=PM360, CN=PM360
序列号: 0x3463b385
哈希算法: sha256
证书MD5: f203b5c84b2e1bc1b3ec64d560fe5f61
证书SHA1: 62e79b39f997f1c9fda76f45386bb41a01171e81
证书SHA256: dd944b6f49178b647286c2f57918ed06127345fce341c9513f43f79356fedb1c
证书SHA512:
fc131ee1d2521e03e6c041f2944ef9c7dddc813b602eef0796b418d77331ea4044da34ccb95a3f5db6d9b04a7cbf9e21633fe1613c3b21da277ee2d34b1a4355

公钥算法: rsa
密钥长度: 2048
指纹: d425e5e5601224d1f34fb37ac972a78edf9333a249bd8b158403ebf32e9af661
找到 1 个唯一证书

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
android.permission.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
android.permission.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储。
android.permission.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
android.permission.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
android.permission.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
android.permission.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
android.permission.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
android.permission.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
android.permission.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
android.permission.READ_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
android.permission.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
android.permission.ACCESS_WIFI_STATE	普通	查看Wi-Fi状态	允许应用程序查看有关Wi-Fi状态的信息。

android.permission.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户错略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
android.permission.BROADCAST_PACKAGE_ADDED	签名	接收新增APP的通知	它允许一个应用程序接收到其他应用程序添加新包（即新安装的可执行文件）的广播消息。
android.permission.BROADCAST_PACKAGE_CHANGED	签名	接收APP变化的通知	它允许一个应用程序接收到其他应用程序变化（安装、卸载、修改）的广播消息。
android.permission.BROADCAST_PACKAGE_INSTALL	签名	接收APP安装的通知	它允许一个应用程序接收到其他应用程序安装新包（即新安装的可执行文件）的广播消息。
android.permission.BROADCAST_PACKAGE_REPLACED	签名	接收APP替换的通知	它允许一个应用程序接收到其他应用程序被覆盖安装的广播消息。
android.permission.RESTART_PACKAGES	普通	重启进程	允许程序自己重启或重启其他程序
android.permission.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.pm360.superepip.ui.activity.TokenLoginActivity	Schemes: crppms://,

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全合规分析

高危: **0** | 警告: **1** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序已使用代码签名证书进行签名

Manifest 配置安全分析

高危: **22** | 警告: **9** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 4.1-4.1.2, [minSdk=16]	信息	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
3	Activity (com.pm360.superepip.ui.activity.WelcomeActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
4	Activity （com.pm360.superepip.ui.activity.WelcomeActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (23) 更新到 28 或更高版本以在平台级别修复此问题。
5	Activity (com.pm360.superepip.ui.activity.MainActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
6	Activity （com.pm360.superepip.ui.activity.MainActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (23) 更新到 28 或更高版本以在平台级别修复此问题。
7	Activity (com.pm360.superepip.ui.activity.LoginActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
8	Activity （com.pm360.superepip.ui.activity.LoginActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (23) 更新到 28 或更高版本以在平台级别修复此问题。
9	Activity (com.pm360.superepip.ui.activity.TokenLoginActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
10	Activity （com.pm360.superepip.ui.activity.TokenLoginActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (23) 更新到 28 或更高版本以在平台级别修复此问题。
11	Activity (com.pm360.superepip.ui.activity.TokenLoginActivity) 未被保护。存在 [intent-filter]。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
12	Activity (com.pm360.superepip.ui.activity.TodoListActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。

13	Activity （com.pm360.superepip.ui.activity.TodoListActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (23) 更新到 28 或更高版本以在平台级别修复此问题。
14	Activity (com.pm360.superepip.ui.activity.NotifiListActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
15	Activity （com.pm360.superepip.ui.activity.NotifiListActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (23) 更新到 28 或更高版本以在平台级别修复此问题。
16	Activity (com.pm360.superepip.ui.activity.SummaryListActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
17	Activity （com.pm360.superepip.ui.activity.SummaryListActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (23) 更新到 28 或更高版本以在平台级别修复此问题。
18	Activity (com.pm360.superepip.ui.activity.WeeklyListActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
19	Activity （com.pm360.superepip.ui.activity.WeeklyListActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (23) 更新到 28 或更高版本以在平台级别修复此问题。
20	Activity (com.pm360.superepip.ui.activity.NewsListActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
21	Activity （com.pm360.superepip.ui.activity.NewsListActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (23) 更新到 28 或更高版本以在平台级别修复此问题。
22	Activity (com.pm360.superepip.ui.activity.PicListActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
23	Activity （com.pm360.superepip.ui.activity.PicListActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (23) 更新到 28 或更高版本以在平台级别修复此问题。

本报告由南明离火移动安全分析平台生成

24	Activity (com.pm360.superepip.ui.activity.ProDocListActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
25	Activity （com.pm360.superepip.ui.activity.ProDocListActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (23) 更新到 28 或更高版本以在平台级别修复此问题。
26	Service (com.pm360.superepip.ui.service.NotifiService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
27	Broadcast Receiver (com.umeng.message.SystemReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
28	Broadcast Receiver (com.umeng.message.MessageReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
29	Broadcast Receiver (com.umeng.message.ElectionReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
30	Broadcast Receiver (com.umeng.message.UmengMessageBootReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
31	Service (com.umeng.message.UmengService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
32	Service (com.umeng.message.UmengMessageIntentReceiverService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

代码安全漏洞检测

高危: **1** | 警告: **5** | 信息: **1** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限

2	应用程序记录日志信息,不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
3	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
4	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
5	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
6	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
7	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限
8	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限

Native 库安全加固检测

本报告由南明离火移动安全分析平台生成

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY (栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED(裁剪符号表)
1	armeabi/libbspatch.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖，在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

2	armeabi/libtnet-2.0.17.1-agoo.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	11/30	android.permission.CALL_PHONE android.permission.CAMERA android.permission.VIBRATE android.permission.RECEIVE_BOOT_COMPLETED android.permission.READ_PHONE_STATE android.permission.WAKE_LOCK android.permission.WRITE_SETTINGS android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.GET_TASKS android.permission.GET_ACCOUNTS
其它常用权限	7/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.ACCESS_WIFI_STATE

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

恶意域名威胁检测

域名	状态	中国境内	位置信息

hydra.alibaba.com	安全	是	**IP地址:** 140.205.160.4 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
log.umsns.com	安全	否	**IP地址:** 140.205.160.4 **国家:** 美利坚合众国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491805 **查看:** Google 地图
agoodm.m.taobao.com	安全	是	**IP地址:** 140.205.160.4 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
alog.umeng.co	安全	否	No Geolocation information available.
apoll.m.taobao.com	安全	是	**IP地址:** 140.205.160.4 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
adash.m.taobao.com	安全	是	**IP地址:** 140.205.160.4 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
oc.umeng.co	安全	否	No Geolocation information available.
api.m.taobao.com	安全	是	**IP地址:** 140.205.160.4 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
utop.umengcloud.com	安全	是	**IP地址:** 140.205.160.4 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图

w.m.taobao.com	安全	否	**IP地址:** 59.82.31.201 **国家:** 美利坚合众国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
au.umeng.co	安全	否	No Geolocation information available.
upoll.umengcloud.com	安全	是	**IP地址:** 140.205.160.4 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
api.waptest.taobao.com	安全	否	**IP地址:** 100.67.1.238 **国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看:** Google 地图
agoodm.wapa.taobao.com	安全	否	No Geolocation information available.
api.wapa.taobao.com	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• http://msdn2.microsoft.com/en-us/library/bb412d1a.aspx • http://jeroenwijering.com/?item=Flash_Media_Player • https://github.com/umdjs/umd/blob/master/templates/returnExports.js • http://www.adobe.com/go/getflashplayer • http://malsup.com/jquery/media/ • http://dev.dcloud.net.cn/mui • http://www.real.com/player/ • https://github.com/pipwerks/PDFObject • http://www.therossman.org/experiments/wmp_play.html • http://pipwerks.mit-license.org/ • http://perfectionkills.com/global-eval-what-are-the-options/ • http://storage.xuetangx.com/public_assets/xuetangx/PDF/PlayerAPI_v1.0.6.pdf • http://fpdownload.macromedia.com/pub/shockwave/cabs/flash/swflash.cab • http://www.microsoft.com/Windows/MediaPlayer/	自研引擎-A
• 218.17.168.19	自研引擎-M
• http://w.m.taobao.com/ • http://w.m.taobao.com/api/ • http://w.m.taobao.com/api/q? • http://w.m.taobao.com/api/r?	com/alimama/mobile/csdk/umupdate/b/a.java
• 218.17.168.19	com/pm360/superepip/config/AppConfig.java

• 127.0.0.1	com/pm360/superepip/network/Proxy.java
• https://58.42.250.187:8888/super/	com/pm360/superepip/util/GlobalSet.java
• 2.0.17.1	org/android/spdy/SpdyAgent.java
• 10.0.0.172	u/aly/t.java
• 42.120.111.1 • http://adash.m.taobao.com/rest/abtest • http://%s:%d/%s/%s/%d/%s • 10.0.0.172 • http://w.m.taobao.com/api/r? • http://adash.m.taobao.com/rest/sur • http://log.umsns.com/ • http://utop.umengcloud.com/rest/api3.do • 10.0.0.200 • http://100.69.165.28/agoo/report • 2.0.17.1 • http://w.m.taobao.com/api/q? • http://alog.umeng.co/app_logs • 218.17.168.19 • http://api.wapa.taobao.com/rest/api3.do • http://100.69.168.33/agoo/report • http://hydra.alibaba.com/ • http://adash.m.taobao.com/rest/gc • 100.69.168.33 • http://oc.umeng.co/check_config_update • https://58.42.250.187:8888/super/ • http://agoodm.m.taobao.com/agoo/report • 100.69.165.28 • 127.0.0.1 • http://au.umeng.co/api/check_app_update • http://%s:%d%s • http://agoodm.wapa.taobao.com/agoo/report • http://w.m.taobao.com/api/ • http://upoll.umengcloud.com • http://log.umsns.com/share/api/ • 110.75.98.154 • 110.75.120.15 • http://api.waptest.taobao.com/rest/api3.do • 42.120.80.36 • http://apoll.m.taobao.com • http://w.m.taobao.com/ • http://api.m.taobao.com/rest/api3.do	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
bspatch	Google	bspatch library for applying delta patches.
友盟推送	Umeng	基于友盟+全域数据建立精准的消息推送平台，为开发者提供更灵活、更智能、更有效的消息推送方案，有效提升用户粘性，提高 App 活跃度。
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。

第三方追踪器检测

名称	类别	网址
Alimama (formerly AdsMogo)	Advertisement	https://reports.exodus-privacy.eu.org/trackers/338
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

敏感凭证泄露检测

可能的密钥
友盟统计的=> "UMENG_APPKEY" : "568f29fb67e58e843c001bcf"
友盟统计的=> "UMENG_CHANNEL" : "huarun_power_SuperEpip"
友盟统计的=> "UMENG_MESSAGE_SECRET" : "218783646516c9c4415147b4c0e1cd88"
凭证信息=> "com.aviary.android.feather.v1.API_KEY" : "wqfpuau8xvnjtrm4"
"password" : "Password"
"user" : "User"
"private_todo" : "Private"
"project_username" : "Username"

免责声明及风险提示: