南明离火
移动应用检测平台

ANDROID 静态分析报告

SoftBankセキュリティ • v17.99.25

分析日期: 2025-03-11 14:41:45

i应用概览

文件名称:	Softbank2023.apk1687866214.0667603.apk
文件大小:	2.2MB
应用名称:	SoftBankセキュリティ
软件包名:	olmpmvfnrsastn.mommliidi.jnhhycgcerqyc
主活动:	olmpmvfnrsastn.mommliidi.jnhhycgcerqyc.icevdagmtujjk
版本号:	17.99.25
最小SDK:	19
目标SDK:	29
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	47/100 (中风险)
杀软检测:	16 个杀毒软件报毒
MD5:	1577e9ac4b2a89be09d0638aac163adc
SHA1:	54f8892ad9730d715735b2db37[illegible]1703691f04b
SHA256:	bf612a2f6201b228015f9[illegible]0585e3d2c1fb5[illegible]e40eb9858f6e23f33

分析结果严重性

高危	中危	信息	安全	关注
4	2	1	2	0

四大组件信息

Activity组件：8个，其中export的有：2个
Service组件：7个，其中export的有：3个
Receiver组件：5个，其中export的有：5个
Provider组件：3个，其中export的有：1个

证书信息

二进制文件已签名
v1 签名: True

v2 签名: True
v3 签名: True
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d7958704d89b7711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
找到 1 个唯一证书

☰ 应用权限

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.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.READ_CONTACTS	危险	读取联系人信息	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
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.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收短信。 恶意程序会在用户未知的情况下监视或删除。
android.permission.REORDER_TASKS	危险	对正在运行的应用程序重新排序	允许应用程序将任务移至前端和后台。恶意应用程序可借此强行进入前端，而不受您的控制。
android.permission.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入手机或 SIM 卡中存储的短信。恶意应用程序可借此删除您的信息。
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息，给您带来费用。
android.permission.RECEIVE_MMS	危险	接收彩信	允许应用程序接收和处理彩信。恶意应用程序可借此监视您的信息，或者将信息删除而不向您显示。
android.permission.READ_PHONE_NUMBERS	危险	允许读取设备的电话号码	允许读取设备的电话号码。这是READ PHONE STATE授予的功能的一个子集，但对即时应用程序公开。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）

android.permission.USE_FULL_SCREEN_INTENT	普通	全屏通知	Android 10以后的全屏 Intent 的通知。
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.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
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。
android.permission.AUTHENTICATE_ACCOUNTS	危险	作为帐户身份验证程序	允许应用程序使用 AccountManager 的帐户身份验证程序功能，包括创建帐户以及获取和设置其密码。
android.permission.WRITE_SYNC_SETTINGS	危险	修改同步设置	允许应用程序修改同步设置。

可浏览的Activity组件

ACTIVITY	INTENT
olmpmvfnrsastn.mommliidi.jnhhycgcerqyc.uysoihunrqkcby	Schemes: smsto://, mms://, mmsto://,

网络通信安全

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

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。

证书安全分析

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	应用程序使用代码签名证书进行签名

MANIFEST分析

高危: **3** | 警告: **16** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/jafmrtkea]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
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	Broadcast Receiver (olmpmvfnrsastn.mommliidi.jnhhycgcerqyc.tugeflzirrhisz$MyReceiver) 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。

4	Broadcast Receiver (olmpmvfnrsastn.mommliidi.jnhhycgcerqyc.emrtfathjdakgv) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BROADCAST_SMS [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
5	Broadcast Receiver (olmpmvfnrsastn.mommliidi.jnhhycgcerqyc.emwpejguuv) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BROADCAST_WAP_PUSH [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
6	Service (olmpmvfnrsastn.mommliidi.jnhhycgcerqyc.qichjivvsrjlnzw) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.SEND_RESPOND_VIA_MESSAGE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
7	Activity设置了TaskAffinity属性 (olmpmvfnrsastn.mommliidi.jnhhycgcerqyc.icevdagmtujjk)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
8	Activity (olmpmvfnrsastn.mommliidi.jnhhycgcerqyc) 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。
9	Activity-Alias (olmpmvfnrsastn.mommliidi.jnhhycgcerqyc) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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。
10	Activity (olmpmvfnrsastn.mommliidi.jnhhycgcerqyc.uysoihunrqkcbyv) 未被保护。 存在一个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。
11	Broadcast Receiver (olmpmvfnrsastn.mommliidi.jnhhycgcerqyc.awgixkzl) 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。
12	Activity (olmpmvfnrsastn.mommliidi.jnhhycgcerqyc.oavtbvxpnd) 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设置了TaskAffinity属性 (olmpmvfnrsastn.mommliidi.jnhhycgcerqyc.uqwojzablgfofcs.nwckokxaypjoex)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
14	Activity设置了TaskAffinity属性 (olmpmvfnrsastn.mommliidi.jnhhycgcerqyc.kkfnueqxnksog)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
15	Activity (smtkbkh.czwak.yosora.mhsjge.pigeb) 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。
16	Service (smtkbkh.czwak.yosora.wxsryvz.yeczph) 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。
17	Broadcast Receiver (smtkbkh.czwak.yosora.wecakufj.rqfdgf) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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。
18	Service (smtkbkh.czwak.yosora.wxsryvz.reofjnwg) 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。
19	Content Provider (smtkbkh.czwak.yosora.uimfizc.wptep) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
20	高优先级的Intent （999） -{1} 个命中 [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。

</> 安全漏洞检测

高危: **0** | 警告: **4** | 信息: **1** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限

3	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
4	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
5	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
6	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限

动态库分析

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	arm64-v8a/librakk.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	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	True info 二进制文件有以下加固函数: ['__strcat_chk', '__strcpy_chk']	True info 符号被剥离

行为分析

编号	行为	标签	文件
00035	查询已安装的包列表	反射	升级会员：解锁高级权限
00193	发送短信	短信	升级会员：解锁高级权限
00038	查询电话号码	信息收集	升级会员：解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00189	获取短信内容	短信	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00052	删除内容 URI 指定的媒体（SMS、CALL_LOG、文件等）	短信	升级会员：解锁高级权限
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00050	Q查询短信服务中心时间戳	短信 信息收集	升级会员：解锁高级权限

00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00075	获取设备的位置	信息收集 位置	升级会员：解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	10/30	android.permission.READ_PHONE_STATE android.permission.READ_CONTACTS android.permission.CALL_PHONE android.permission.READ_SMS android.permission.RECEIVE_SMS android.permission.WRITE_SMS android.permission.SEND_SMS android.permission.RECEIVE_MMS android.permission.RECEIVE_BOOT_COMPLETED android.permission.GET_ACCOUNTS
其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.REORDER_TASKS android.permission.FOREGROUND_SERVICE android.permission.AUTHENTICATE_ACCOUNTS

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。

URL链接分析

URL信息	源码文件
• https://github.com/grandcentrix/tray/issues • https://github.com/grandcentrix/tray/wiki/custom-authority	ehkuubwvsa/akfcezpoh/akfcezpoh/hsoepucwpjf/ouateotj.java

第三方SDK

SDK名称	开发者	描述信息
Jetpack App Startup	Google	App Startup 库提供了一种直接，高效的方法来在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。

密钥凭证

可能的密钥
"tray__authority" : "legacyTrayAuthority"
IgMXGQEaB0FHXVFTXDkGAgkfGgVGICZTV11FVU87IidbQl1OAAVbQUdAX0VNNwgVDQRNQVFCRF5eXFxQKx8UCxQeGVxQXUFc
BQ0bER4VFAcCB1sAERouDw4fGBgSRlU=
iuP8lNLXgO/dVRIGFw0KHx5K
ifXDme3sj+7olP7Wks7gSory1JPh1Q==
DgIJAgIfAkACFhMeHR0cBQIeQyQjLzYsMTs7ICozPiQsIiM=
DgIJAgIfAkACFhMeHR0cBQIeQyQjLTc6NzYrPSI/
BxgZAFdZSRodHQYJHAcDDQNeGRkWQR4cBhxaHgEL
DgIJAgIfAkACFhMeHR0cBQIeQyQjLzYsIjw6Oi4vOCM=
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
DgIJAgIfAkACAQ4FHQoKHkMkCBoDHhocDwpaPSI/MiIoNSMnJDYI
iefLluXcgfHfl97SUg0DAX4VEQrUGxc=
DgIJAgIfAkAbHRUWGhpBDQ4EBBkIQCIyIjg1KSozLBQpMyI=
DgIJAgIfAkAbHRUWGhpBDQ4EBBkIQDA2IiciLSAhPTwoIiMq
DgIJAgIfAkAbHRUWGhpBDQ4EBBkICDY2LTYgKw==
DgIJAgIfAkACAQ4FHQoKHkMkCBoDHhocDwpaLyw4JD8jKSUmMz0mNisqKiosJSEi
DgIJAgIfAkAbHRUWGhpBDQ4EBBkIQCIyIjg1KSozPzUgOTArNg==
DgIJAgIfAkACEhMeHR0cBQIeQyQjLzYsMj4n

免责声明及风险提示: