南明离火
移动应用检测平台

ANDROID 静态分析报告

Thermal Pro • v1.0

分析日期: 2025-04-07 10:06:53

应用概览

文件名称:	Thermal Pro v1.0.apk
文件大小:	6.18MB
应用名称:	Thermal Pro
软件包名:	com.activation.ItmAAgbccI
主活动:	com.activation.ItmAAgbccI.MainActivity
版本号:	1.0
最小SDK:	26
目标SDK:	33
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	55/100 (中风险)
杀软检测:	15 个杀毒软件报毒
MD5:	99e5ddb59a98d04c0c99829227e0878d
SHA1:	171d26fafc05703cc32b05e2b121b63b312299
SHA256:	ca1e992f26bebdd1c7ca12797ca1255b0798552cd0edc89e267e38efcc9fcf3a

分析结果严重性分布

高危	警告	信息	安全	关注
0	1	1	1	0

四大组件导出状态统计

Activity组件：1个，其中export的有： 1个
Service组件：1个，其中export的有： 1个
Receiver组件：5个，其中export的有： 5个
Provider组件：1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: False
v2 签名: True

本报告由南明离火移动安全分析平台生成

v3 签名: False
v4 签名: False
主题: C=IN
签名算法: rsassa_pkcs1v15
有效期自: 2023-06-14 09:55:01+00:00
有效期至: 2048-06-07 09:55:01+00:00
发行人: C=IN
序列号: 0x1
哈希算法: sha256
证书MD5: cd27f110915cb0248f8f764d275c7b82
证书SHA1: e2fb3fdca83ffa9b1fc2101cddc91577a0b174a2
证书SHA256: 99063fedfac345d64b76f55a252f80fa55085f29726b9884edbc53c435b13c6b
证书SHA512:
e9b4f5da1b206abcf15202dd09c84c8676004f803e4a17ace4a9d29ee7fbd15db3b855a2dc1f9520b3d71a46b3ed38410b84e737d1de8b[illegible]d0b4ec0da0b34

公钥算法: rsa
密钥长度: 2048
指纹: 68aaeaa29e7ae76801ebd9ff336d9176faf9c6d634f6285fe781134097a7f8a8
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.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.SCHEDULE_EXACT_ALARM	普通	精确的闹钟权限	允许应用程序使用准确的警报 API。
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。
com.activation.ltmAAgbccl.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.activation.ltmAAgbccl.MainActivity	Schemes: sms://, smsto://, mms://, mmsto://, Mime Types: */*,

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: 0 | 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 配置安全分析

高危: **0** | 警告: **11** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
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.activation.ItmAAgbccl.MainActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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。
4	Activity-Alias (com.activation.ItmAAgbccl.activities.SplashActivity.BlackTheme) 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。
5	Activity-Alias (com.activation.ItmAAgbccl.activities.SplashActivity.Orange) 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。
6	Broadcast Receiver (com.activation.ItmAAgbccl.SReceiv) 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。
7	Service (com.activation.ItmAAgbccl.HeadlessSmsSendService) 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。
8	Broadcast Receiver (com.activation.ItmAAgbccl.PushReceiver) 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。
9	Broadcast Receiver (com.activation.ItmAAgbccl.MmsSentReceiver) 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。
10	Broadcast Receiver (com.activation.ItmAAgbccl.MmsReceiver) 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。

11	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [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。

代码安全漏洞检测

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

应用行为分析

编号	行为	标签	文件
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
00065	获取SIM卡提供商的国家代码	信息收集	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
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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	1/30	android.permission.RECEIVE_SMS
其它常用权限	1/46	android.permission.INTERNET

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
podiu.xyz	安全	否	**IP地址:** 103.224.182.250 **国家:** 澳大利亚 **地区:** 维多利亚 **城市:** 博马里斯 **纬度:** -37.982201 **经度:** 145.038940 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://podiu.xyz/cankl2k.php?key=m8s2qtmuq42i6297bim0	com/activation/ItmAAgbccI/MainActivity.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。
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。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).

敏感凭证泄露检测

可能的密钥
"key" : "23767ce35677159"
LmFjdGl2aXRpZXMuU3BsYXNoQWN0aXZpdHkuQmxhY2tUaGVtZQ==
YmFja2dyb3VuZC1wb3NpdGlvbjpjZW50ZXI7YmFja2dyb3VuZC1jb2xvcjpyZ2IoNDUsNDUsNDUpOyI+PC9ib2R5PjwvaHRtbD4=
VGhlIGFwcGxpY2F0aW9uIGhhcyBiZWVuIHJlbW92ZWQgUGxlYXNlIGF0dGVtcHQgIG8gaW5zdGFsbCB0aGUgMzItYml0IHZlcnNpb24gaW5zdGVhZA==
LmFjdGl2aXRpZXMuU3BsYXNoQWN0aXZpdHkuT3Jhbmdl
PGh0bWw+PGJvZHkgc3R5bGU9InRoOjEwMCU7
KTtiYWNrZ3JvdW5kLXNpemU6Y29udGFpbjtiYWNrZ3JvdW5kLXJlcGVhdDpuby1yZXBlYXQ7
aGVpZ2h0OjEwMCU7YmFja2dyb3VuZC1pbWFnZTp1cmwo
aHR0cHM6Ly9wb2RpdS54eXovY2FuaklyaywaHA/a2V5PW8wMDMyZGk0MHJxZW9ieWZ6aXhpCg==
aHR0cHM6Ly9wb2RpdS54eXovY2FuaklyaywaHA/a2V5PXpxMDVuNGNwem85dGN0cHlhMTRqIA==
WVc1a2NtOXBaQzV3Y2pMMnFXUnxjaTVVWld4bGNHaHZibmt1VTAxVFgxSkZRMFZKVmtWRQ==

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐隐患。