南明离火
移动应用检测平台

ANDROID 静态分析报告

□□□ • v1.4.7

本报告由南明离火移动安全分析平台生成

分析日期: 2024-09-28 14:41:56

i应用概览

文件名称:	8822b46b35d5f193bd2ca7dd994c9c5325ae2f122f6a660a5df6d3132c7428eb.apk
文件大小:	2.46MB
应用名称:	□□□
软件包名:	bbbheegb.cbfdhhfc.ieffdbdd
主活动:	bbbheegb.cbfdhhfc.ieffdbdd.wefreg.erwgler.ssfskdekvgrfd
版本号:	1.4.7
最小SDK:	26
目标SDK:	29
加固信息:	未加壳
应用程序安全分数:	52/100 (中风险)
杀软检测:	23 个杀毒软件报毒
MD5:	f415954942a1a8e404b5f2fa6c4f86bd
SHA1:	683938ed353e84ea26176ad274552ad6f108b430
SHA256:	8822b46b35d5f193bd2ca7dd994c9c5325ae2f122f6a660a5df6d3132c7428eb

分析结果严重性

高危	中危	信息	安全	关注
1	5	10	1	0

四大组件信息

Activity组件：2个，其中export的有：2个
Service组件：4个，其中export的有：1个
Receiver组件：1个，其中export的有：0个
Provider组件：1个，其中export的有：0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=9f83, ST=9f83, L=9f83, O=9f83, OU=9f83, CN=9f83
签名算法: rsassa_pkcs1v15
有效期自: 2024-05-15 02:30:03+00:00
有效期至: 2029-11-05 02:30:03+00:00
发行人: C=9f83, ST=9f83, L=9f83, O=9f83, OU=9f83, CN=9f83
序列号: 0x454a44b9
哈希算法: sha256
证书MD5: 32dc43bc690d4460b29c5c711df72f1f
证书SHA1: 778a0639d4e3037237173871c1a0913dd59690e3
证书SHA256: 3f24909b0bc5b24f0e92dd5735ac32c8d9fe4855b27eab6c7105bef1b2d6bd1e
证书SHA512:
fc63b88c9ef9b1e74739230a308c9d2651a74f1568bc7595faabca310ac6890b351f939cd7ec77025df38ff9c811fdc3001436121986697f32beb46152ecf14c

公钥算法: rsa
密钥长度: 2048
指纹: ef65bf72a22918044685ca59d694af5933ee3486856597a088e57c3d0f356da0
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.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.READ_CONTACTS	危险	读取联系人信息	允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.WRITE_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。
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.GET_ACCOUNTS_PRIVILEGED	签名(系统)	授予对帐户服务的访问权限	允许访问帐户服务中的帐户列表。
android.permission.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加、删除帐户及删除其密码之类的操作。
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.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_PROFILE	危险	读取用户资料	允许应用程序读取用户个人信息。
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.WRITE_PROFILE	危险	写入用户资料	允许应用程序 读写用户个人信息。
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.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
android.permission.NFC	危险	控制nfc功能	允许应用程序与支持nfc的物体交互。

本报告由南明离火移动安全分析平台生成

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.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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.USE_CREDENTIALS	危险	使用帐户的身份验证凭据	允许应用程序请求身份验证标记。
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.READ_SYNC_SETTINGS	普通	读取同步设置	允许应用程序读取同步设置，例如是否为 联系人 启用同步。
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。
com.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
android.permission.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
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.READ_CALENDAR	危险	读取日历活动	允许应用程序读取您手机上存储的所有日历活动。恶意应用程序可借此将您的日历活动发送给其他人。
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。
com.android.voicemail.permission.READ_VOICEMAIL	未知	未知权限	来自 android 引用的未知权限。
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。
android.permission.READ_SYNC_STATS	普通	读取同步统计信息	允许应用程序读取同步统计信息；例如已发生的同步历史记录。
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.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）

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	应用程序已使用代码签名证书进行签名

MANIFEST分析

高危: **0** | 警告: **5** | 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存在漏洞的 Android 版本上 Android 8.0, minSdk=26]	信息	该应用程序可以安装在具有多个漏洞的旧版本 Android 上。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	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。
3	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/a]	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。
4	Activity-Alias (bbbheegb.cbfdhhfc.ieffdbdd.alias) 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 (bbbheegb.cbfdhhfc.ieffdbdd.wefreg.erwgler.ergvfrledblr) 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。
6	Service (bbbheegb.cbfdhhfc.ieffdbdd.XAKeepaliveZZ.service.AAPlayerMusicServiceZZ) 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。
7	高优先级的Intent (2147483647) [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

序号	问题	等级	参考标准	文件位置

敏感权限分析

类型	匹配	权限
恶意软件常用权限	14/30	android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS android.permission.GET_ACCOUNTS android.permission.CALL_PHONE android.permission.SYSTEM_ALERT_WINDOW android.permission.READ_PHONE_STATE android.permission.WAKE_LOCK android.permission.WRITE_SETTINGS android.permission.VIBRATE android.permission.READ_CALL_LOG android.permission.READ_SMS android.permission.READ_CALENDAR android.permission.SEND_SMS android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	8/46	android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.READ_EXTERNAL_STORAGE com.android.launcher.permission.INSTALL_SHORTCUT android.permission.FOREGROUND_SERVICE

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。

第三方SDK

SDK名称	开发者	描述信息
MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高，稳定性强。

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。