南明离火
移动应用检测平台

ANDROID 静态分析报告

□□□ □□□□. • v30.2.3.18

分析日期: 2025-04-26 19:04:24

应用概览

文件名称:	□□□ □□□□. v30.2.3.18.apk
文件大小:	2.19MB
应用名称:	□□□ □□□□.
软件包名:	derewr.sdfvwefwe.sdwrf
主活动:	DDDuiKKK.DDDSplashActivityKKK
版本号:	30.2.3.18
最小SDK:	26
目标SDK:	31
加固信息:	梆梆安全
开发框架:	Java/Kotlin
应用程序安全分数:	54/100 (中风险)
杀软检测:	20 个杀毒软件报毒
MD5:	1f4b8fb24c6a37675fc2b3df8f63d93b
SHA1:	445bb21f6f6f2dbb6379de4145d67[illegible]da380d
SHA256:	3ca157f865a26d16704614db950[illegible]845865e8c95adc7741b42a8ba71075574f8

分析结果严重性

高危	中危	信息	安全	关注
2	3	1	2	0

四大组件信息

Activity组件：2个，其中export的有：1个
Service组件：2个，其中export的有：0个
Receiver组件：2个，其中export的有：2个
Provider组件：2个，其中export的有：0个

证书信息

二进制文件已签名
v1 签名: False
v2 签名: True

v3 签名: False
v4 签名: False
主题: C=KR, ST=idoslkskskslslw, L=kxkkslwllwlwlww, O=xiosjenmwwm, OU=awmmqmmqlwl, CN=jwnwwmwmi9
签名算法: rsassa_pkcs1v15
有效期自: 2024-09-20 00:42:01+00:00
有效期至: 2074-09-08 00:42:01+00:00
发行人: C=KR, ST=idoslkskskslslw, L=kxkkslwllwlwlww, O=xiosjenmwwm, OU=awmmqmmqlwl, CN=jwnwwmwmi9
序列号: 0x2e28182c
哈希算法: sha256
证书MD5: 435ee4a1807531a10fb2f64a5ba8e8bf
证书SHA1: ee54403a59103d01b0cd1e12ecbe6f5b1ab4699f
证书SHA256: bd7478aa8b5c53dee65ecdd78cbd3fb820b3a045dc8d02022ac9e19074b40607
证书SHA512:
abc7b0c94064acbd30490859fbe5106d3f80d4da4ed6c160d996758196c898ccd74690cbc372463e7067d1ca3b00084c0112d238077bdcb689e7e58b3a772e60b

公钥算法: rsa
密钥长度: 2048
指纹: 58fe888d43586491b30272bdb49769cd5ebd48bbb17faa378fd2e4b8ddade75b
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.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.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.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.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_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.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.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.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。
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.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.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。

本报告由南明离火移动安全分析平台生成

android.permission.DEVICE_POWER	签名	开机或关机	允许应用程序启动/关闭设备。
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.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.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
com.android.alarm.permission.SET_ALARM	未知	未知权限	来自 android 引用的未知权限。
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。

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: **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分析

高危: **1** | 警告: **4** | 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/network_security_config]	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	程序可被任意调试 [android:debuggable=true]	高危	应用可调试标签被开启，这使得逆向工程师更容易将调试器挂接到应用程序上。这允许导出堆栈跟踪和访问调试助手类。
3	Activity-Alias (DDDuiKKK.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。
4	Broadcast Receiver (DDDReceiverKKK.DDDMainReceiverKKK) 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。
5	Broadcast Receiver (DDDReceiverKKK.DDDAlarmReceiverKKK) 受权限保护，但是应该检查权限的保护级别。 Permission: com.android.alarm.permission.SET_ALARM [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	高优先级的Intent （2147483647） - {2} 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: **0** | 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	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

行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00024	Base64解码后写入文件	反射 文件	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
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
00202	打电话	控制	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
00203	将电话号码放入意图中	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
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
00094	连接到 URL 并从中读取数据	命令 网络	升级会员：解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限
00192	获取短信收件箱中的消息	短信	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

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
00115	获取设备的最后已知位置	信息收集 位置	升级会员：解锁高级权限
00112	获取日历事件的日期	信息收集 日历	升级会员：解锁高级权限
00078	获取网络运营商名称	信息收集 电话服务	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
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00083	查询IMEI号	信息收集 电话服务	升级会员：解锁高级权限
00132	查询ISO国家代码	电话服务 信息收集	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
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
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
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00049	查询短信发送者的电话号码	短信 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
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
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
00072	将 HTTP 输入流写入文件	命令 网络 文件	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	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	7/30	android.permission.READ_SMS android.permission.SEND_SMS android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS android.permission.READ_PHONE_STATE android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK
其它常用权限	6/46	android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.FOREGROUND_SERVICE android.permission.ACCESS_NETWORK_STATE 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。

域名检测

域名	状态	中国境内	位置信息
funeral.snuh.org	安全	否	**IP地址:** 203.229.136.49 **国家:** 大韩民国 **地区:** 京畿道 **城市:** 城南市 **纬度:** 37.420624 **经度:** 127.126717 **查看:** Google 地图

URL链接分析

URL信息	源码文件
• http://103.13.222.5/index.html	e/e.java
• https://funeral.snuh.org/main.do	DDDuiKKK/DDDMainActivityKKK.java
• https://github.com/qwdqwddqw/qwdqwddqw/commit/90e94a664d95e5ed135cc94377e14abf5d6af43e	DDDserviceKKK/DDDMainServiceKKK.java

第三方SDK

SDK名称	开发者	描述信息
梆梆安全	梆梆安全	针对目前移动应用普遍存在的破解、篡改、盗版、钓鱼欺诈、内存调试、数据窃取等各类安全风险，梆梆安全为开发者提供全面的移动应用加固加密技术和攻击防范服务。
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。

密钥凭证

可能的密钥
WlJltbL04VPxU2sIwY2EB8rWR49aHQ
96e94a664d95e5ed135cc94377e14abf5d6af43e

免责声明及风险提示: