南明离火
移动应用检测平台

ANDROID 静态分析报告

DISHA_KEB • v2.45

分析日期: 2025-04-10 14:09:46

应用概览

文件名称:	DISHA_KEB v2.45.apk
文件大小:	5.63MB
应用名称:	DISHA_KEB
软件包名:	disha.keb.v3
主活动:	com.android.inputmethod.latin.spellcheck.SpellCheckerSettingsActivity
版本号:	2.45
最小SDK:	8
目标SDK:	14
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	51/100 (中风险)
杀软检测:	12 个杀毒软件报毒
MD5:	ff036ecf3867254c717c057f075abe17
SHA1:	148eca03d5b70c5ee6f482d73692a338039018a6
SHA256:	45dbc6aa19914cb26a3ed8f7ed88fda7ad244b15639761bf615c0488925a51b7

分析结果严重性分布

高危	中危	信息	安全	关注
1	1	1	1	0

四大组件导出状态统计

Activity组件：9个，其中export的有： 2个
Service组件：3个，其中export的有： 2个
Receiver组件：0个，其中export的有： 0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=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:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea3039772720179587704d89b7711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
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.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_USER_DICTIONARY	危险	读取用户定义的词典	允许应用程序读取用户在用户词典中存储的任意私有字词、名称和短语。
android.permission.WRITE_USER_DICTIONARY	普通	写入用户定义的词典	允许应用程序向用户词典中写入新词。
android.permission.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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_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。

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	应用程序使用代码签名证书进行签名

Manifest 配置安全分析

高危: **0** | 警告: **10** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，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。
2	Service (com.android.inputmethod.latin.spellcheck.AndroidSpellCheckerService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_TEXT_SERVICE [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。
3	Service (com.android.inputmethod.latin.DictionaryEditor) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_INPUT_METHOD [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。
4	Activity (com.android.inputmethod.latin.DomainEditor) 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。
5	Activity (com.android.inputmethod.latin.DictionaryEditorDebugSettings) 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。
6	Activity (com.android.inputmethod.latin.PerfectInputLanguageSelection) 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。
7	Activity (com.android.inputmethod.latin.AutoTextEditor) 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。
8	Activity (com.android.inputmethod.latin.CustomDictionaryEditor) 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。
9	Activity (com.android.inputmethod.latin.SlideSelector) 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。
10	Activity (com.android.inputmethod.latin.BackupPro) 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。

代码安全漏洞检测

高危: **1** | 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	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	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

Native 库安全加固检测

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/libjni_latinime_pt2_new.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	No RELRO high 此共享对象未启用 RELRO。整个 GOT（.got 和 .got.plt）都是可写的。如果没有此编译器标志，全局变量上的缓冲区溢出可能会覆盖 GOT 条目。使用选项 -z,relro,-z,now 启用完整 RELRO，仅使用 -z,relro 启用部分 RELRO。	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	True info 符号被剥离

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	3/30	android.permission.VIBRATE android.permission.RECORD_AUDIO android.permission.READ_CONTACTS
其它常用权限	1/46	android.permission.WRITE_EXTERNAL_STORAGE

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。

敏感凭证泄露检测

可能的密钥
"subtype_mode_keyboard" : "tastiera"
"settings_key_mode_auto_name" : "Otomatis"
"key_hight_horizontal" : "key_hight_horizontal"
"gesture_key_up" : "10"
"settings_key_mode_auto_name" : "Automaattinen"
"arrows_keys_hight_vertical" : "arrows_keys_hight_vertical"

本报告由南明离火移动安全分析平台生成

"arrows_keys_hight_horizontal" : "arrows_keys_hight_horizontal"
"settings_key_mode_auto_name" : "Automatic"
"gesture_key_right" : "8"
"settings_key_mode_auto_name" : "Automatique"
"settings_key_mode_auto_name" : "Automatico"
"settings_key_mode_auto_name" : "Automatiskt"
"settings_key_mode_auto_name" : "Automatinis"
"subtype_mode_keyboard" : "Teclado"
"subtype_mode_keyboard" : "teclado"
"settings_key_mode_auto_name" : "Automatisch"
"settings_key_mode_auto_name" : "Otomatik"
"gesture_key_left" : "9"
"subtype_mode_keyboard" : "teclat"
"settings_key_mode_auto_name" : "Automatycznie"
"subtype_mode_keyboard" : "klawiatura"
"settings_key_mode_auto_name" : "Automat"
"settings_key_mode_auto_name" : "Awtomatiko"
"gesture_key_down" : "11"
"subtype_mode_keyboard" : "keyboard"
"subtype_mode_keyboard" : "tangentbord"
"subtype_mode_keyboard" : "toetsenbord"
"settings_key_mode_auto_name" : "Automaticky"
"gesture_close_keyboard" : "3"
"key_hight_vertical" : "key_hight_vertical"
"settings_key_mode_auto_name" : "Automatski"
"subtype_mode_keyboard" : "clavier"
"settings_key_mode_always_show" : "1"
"settings_key_mode_auto_name" : "Automatisk"
"settings_key_mode_always_hide" : "2"
"subtype_mode_keyboard" : "tastatur"

"settings_key_mode_auto_name" : "Automatikus"
"settings_key_mode_auto" : "0"
"sound_on_keypress" : "Knappljud"
"subtype_mode_keyboard" : "Tastatur"
"subtype_mode_keyboard" : "klavye"
"settings_key_mode_auto_name" : "Samodejno"
"subtype_mode_keyboard" : "tipkovnica"

免责声明及风险提示: