南明离火
移动应用检测平台

ANDROID 静态分析报告

8Vim v12

分析日期: 2025-07-05 13:52:27

应用概览

文件名称:	09646bd690646a421de2050b27bcad221fdc3b3b8dcb6d98bf4881b89f124c7d.apk
文件大小:	2.81MB
应用名称:	8Vim
软件包名:	inc.flide.vi8
主活动:	inc.flide.vim8.ui.SettingsActivity
版本号:	12
最小SDK:	21
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:	64/100 (低风险)
杀软检测:	经检测，该文件安全
MD5:	80b03936d4232148ba204527d8c84dda
SHA1:	45ab60dbdc2f0758dcb23ddce02630bacfeca391
SHA256:	09646bd690646a421de2050b27bcad221fdc3b3b8dcb6d98bf4881b89f124c7d

分析结果严重性分布

高危	中危	信息	安全	关注
0	4	1	1	0

四大组件导出状态统计

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

应用签名证书信息

APK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=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2018-08-30 13:24:02+00:00
有效期至: 2048-08-30 13:24:02+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xc06b4030633ba0989535b5de977b83b98245cceb
哈希算法: sha256
证书MD5: b223653802f49f8d3df5e3239a3a233f
证书SHA1: a3887b17caa5a59782c8b40dba6fd275f87f8068
证书SHA256: 1d602ba41fe0265d8a5c3028006fcb923e4e459287def1f745e74b88462fb9e3
证书SHA512:
46cee9bfddef2749593e2cebff6839584a1979b273e002541a171e7374b6fb9281606103f54f8489dd5a35067[illegible]c644762c36b89ec00359[illegible]ef55393174c2fb3

公钥算法: rsa
密钥长度: 4096
指纹: 220e2743aaffd4ad75d5a52d9f3ef45e08e6ad92134885a43465fa9ae36e094f
共检测到 1 个唯一证书

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	应用已使用代码签名证书进行签名。

Manifest 配置安全分析

高危: **0** | 警告: **2** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	Service (inc.flide.vim8.MainInputMethodService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_INPUT_METHOD [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

2	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

代码安全漏洞检测

高危: **0** | 警告: **1** | 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
2	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

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
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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	0/30	
其它常用权限	0/46	

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
yaml.org	安全	否	**IP地址:** 185.199.109.153 **国家:** 美国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图
twitter.com	安全	否	**IP地址:** 172.66.0.227 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
app.element.io	安全	否	**IP地址:** 185.199.109.153 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
8vim.com	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• https://play.google.com/store/apps/details?id=inc.flide.vi8	inc/flide/vim8/ui/SettingsActivity.java
• https://github.com/flide/8vim • https://twitter.com/8vim_?s=09 • https://app.element.io/#/room/#8vim/lobby:matrix.org • https://8vim.com • https://play.google.com/store/apps/details?id=inc.flide.vi8	inc/flide/vim8/ui/AboutUsActivity.java
• https://yaml.org/spec/1.1/#id934537	p3/a.java

第三方 SDK 组件分析

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。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。

邮箱地址敏感信息提取

EMAIL	源码文件
flideravi@gmail.com	inc/flide/vim8/ui/SettingsActivity.java

敏感凭证泄露检测

可能的密钥
"pref_board_bg_color_key" : "board_bg_color"
"pref_board_fg_color_key" : "board_fg_color"
"pref_circle_x_offset_key" : "x_board_circle_centre_x_offset"
"pref_circle_y_offset_key" : "x_board_circle_centre_y_offset"
"pref_display_sector_icons_key" : "user_preferred_display_icons_in"
"pref_display_wheel_characters_key" : "user_preferred_display_letters_on_wheel"
"pref_haptic_feedback_key" : "user_preferred_haptic_feedback_enabled"
"pref_random_trail_color_key" : "user_preferred_random_trail_color_enabled"
"pref_select_custom_keyboard_layout_key" : "select_custom_keyboard_layout"
"pref_select_emoji_keyboard_key" : "select_emoji_keyboard"
"pref_select_keyboard_layout_key" : "select_keyboard_layout"
"pref_selected_custom_keyboard_layout_uri" : "pref_selected_custom_keyboard_layout_uri"
"pref_selected_emoticon_keyboard" : "selected_emoticon_keyboard"
"pref_selected_keyboard_layout" : "selected_keyboard_layout"
"pref_sidebar_left_key" : "user_preferred_sidebar_left"
"pref_sound_feedback_key" : "user_preferred_sound_feedback_enabled"
"pref_trail_color_key" : "trail_color"
"pref_typing_trail_visibility_key" : "user_preferred_typing_trail_visibility"
"pref_use_custom_selected_keyboard_layout" : "use_custom_selected_keyboard_layout"

Google Play 应用市场信息

标题: 8vim Keyboard

评分: 4.24 **安装:** 5,000+ **价格:** 0 **Android**版本支持: **分类:** 效率 **Play Store URL:** inc.flide.vi8

开发者信息: flide inc., flide+inc., None, https://github.com/flide/8VIM, 8vim@protonmail.com,

发布日期: 2023年3月29日 隐私政策: Privacy link

关于此应用:

8vim是一种开放源代码的小屏幕键盘，旨在克服小的键入空间的局限性，并为用户提供工具，使他/她正在键入的任何文本框都具有全文编辑器样式的编辑功能。 可用性指南 那么，8Vim有什么功能呢？一旦您知道如何使用此东西打字（了解如何使用此原始的[8Pen-game App]打字（https://play.google.com/store/apps/details?id=com.eightpen.android.wordcup&hl= zh），您必须了解以下内容 基本所需的东西 右扇区充当退格键。 底部扇区充当Enter键。 顶部扇区是SHIFT和CAPS_LOCK键的组合，即，按一次Shift键处于活动状态，按一次两次CAPS处于活动状态，再按一次则一切恢复正常。 左扇区用作将您带到数字键盘的按钮。 光标移动 如果将手指从中心圆移动到任何扇形并停留，则将模拟光标移动。例如，如果您从圆->向右滑动，则光标将向右移动。您得到图片。 选拔 键盘中内置有选择项。如果您将手指从右扇形移动到圆圈，则光标将开始向右移动并选择路径中的所有内容。释放后，将打开一个选择键盘以执行各种愚蠢操作。 粘贴功能 从右->圆形->抬起手指移动手指进行粘贴。剪贴板中的任何内容。 该项目的源代码可以在github上找到：https://github.com/flide/8VIM

免责声明及风险提示:

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。