南明离火
移动应用检测平台

ANDROID 静态分析报告

zs cms • v3.0

分析日期: 2025-03-11 15:13:47

应用概览

文件名称:	isskct.vfyndo.qeffkv.apk
文件大小:	27.73MB
应用名称:	zs cms
软件包名:	isskct.vfyndo.qeffkv
主活动:	com.westpm.hlahl.ui.activity.OpeningActivity
版本号:	3.0
最小SDK:	16
目标SDK:	30
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	49/100 (中风险)
杀软检测:	AI评估：安全
MD5:	1e4461ac14c8630661f59d503c36422d
SHA1:	c1a75cadf6ef47569724cc3072c[illegible]ad0f408e1
SHA256:	b61fcc02d99b5c41b99c[illegible]b81d695fd880c242fa9[illegible]aa388fc855ef7297ba

分析结果严重性

高危	中危	信息	安全	关注
3	7	1	2	4

四大组件信息

Activity组件：14个，其中export的有：0个
Service组件：0个，其中export的有：0个
Receiver组件：0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: False

v2 签名: True
v3 签名: False
v4 签名: None
主题: C=fvmamscqsmjky, ST=slmmhwnnxjivd, L=zxdejnknuoemm, O=xoy1739969862058, OU=kul1739969862058, CN=TG@apken888
签名算法: rsassa_pkcs1v15
有效期自: 2025-02-19 12:57:42+00:00
有效期至: 2075-02-07 12:57:42+00:00
发行人: C=fvmamscqsmjky, ST=slmmhwnnxjivd, L=zxdejnknuoemm, O=xoy1739969862058, OU=kul1739969862058, CN=TG@apken888
序列号: 0x5f219be4
哈希算法: sha1
证书MD5: c3e5a967f763127895c06121ddcbe82a
证书SHA1: 0c835c0f9f9ac59c19dc006335cda217ec756ba7
证书SHA256: 64061531c27e7cd4dc408160d29807593b589f6cc5f89d347b13ea0609d3b4d8
证书SHA512:
218fbd3c8f160288e768663edd3553b3c8048bb498b6c8c6e0f6ba3b4e91504c545cbcf04ac0756069dd7a699a7d223a69844e014bfcf19ab8d883f45b36acfa

公钥算法: rsa
密钥长度: 1024
指纹: 0dc77d0c556e7ff3a2c6ec30c1e4485e4db02fc39982f62b5ed8da5f300f183f
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.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.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_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.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
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.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.NETWORK_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
android.permission.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
android.permission.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.READ_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
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。
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。

com.android.launcher.permission.UNINSTALL_SHORTCUT	签名	删除快捷方式	这个权限是允许应用程序删除桌面快捷方式。
com.android.launcher.permission.READ_SETTINGS	危险	读取桌面快捷方式	这种权限的作用是允许应用读取桌面快捷方式的设置。
com.android.launcher.permission.WRITE_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	危险	允许从外部存储读取用户选择的图像或视频文件	允许应用程序从用户通过权限提示照片选择器选择的外部存储中读取图像或视频文件。应用程序可以检查此权限以验证用户是否决定使用照片选择器，而不是授予对 READ_MEDIA_IMAGES 或 READ_MEDIA_VIDEO 的访问权限。它不会阻止应用程序手动访问标准照片选择器。应与 READ_MEDIA_IMAGES 和/或 READ_MEDIA_VIDEO 一起请求此权限，具体取决于所需的媒体类型。

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: **0** | 警告: **2** | 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。
3	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。

安全漏洞检测

高危: **2** | 警告: **5** | 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	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
3	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
4	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
5	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
6	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
7	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
8	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限

9	已启用远程WebView调试	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

行为分析

编号	行为	标签	文件
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
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
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
00109	连接到 URL 并获取响应代码	网络 命令	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
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
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00014	将文件读入流并将其放入 JSON 对象中	文件	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
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	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
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
00054	从文件安装其他APK	反射	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
00191	获取短信收件箱中的消息	短信	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

敏感权限分析

类型	匹配	权限
恶意软件常用权限	3/30	android.permission.READ_PHONE_STATE android.permission.CAMERA android.permission.WRITE_SETTINGS
其它常用权限	9/46	android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_AUDIO android.permission.READ_MEDIA_VIDEO com.android.launcher.permission.INSTALL_SHORTCUT

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
ganggan1226.gz.bcebos.com	安全	是	**IP地址:** 121.228.183.252 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
www.migu.cn	安全	是	**IP地址:** 117.135.165.90 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
w-1331615372.cos.ap-guangzhou.myqcloud.com	安全	是	**IP地址:** 27.155.119.179 **国家:** 中国 **地区:** 福建 **城市:** 福州 **纬度:** 26.061390 **经度:** 119.306107 **查看:** 高德地图
guangdong-5.zos.ctyun.cn	安全	是	**IP地址:** 14.215.163.248 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图

URL链接分析

URL信息	源码文件
• https://st-cn.meishij.net/r/112/108/4089612/s4089612_145431725551281.jpg • https://st-cn.meishij.net/r/137/202/3863137/s3863137_142806509977951.jpg • https://st-cn.meishij.net/r/141/154/4351141/s4351141_150509718716126.jpg • https://st-cn.meishij.net/r/207/11/9502957/s9502957_151304147951837.jpg • https://st-cn.meishij.net/r/86/63/1640836/s1640836_151543003415109.jpg • https://st-cn.meishij.net/r/185/123/1655935/s1655935_18695.jpg • https://st-cn.meishij.net/r/115/102/588115/s588115_149347346669780.jpg • https://st-cn.meishij.net/r/147/198/4174647/s4174647_150943807386688.jpg • https://st-cn.meishij.net/r/150/78/3394650/s3394650_149849114659095.jpg • https://st-cn.meishij.net/r/41/203/113291/s113291_154338858269516.jpg • https://st-cn.meishij.net/r/246/109/4089996/s4089996_148768018789201.jpg • https://st-cn.meishij.net/r/150/78/3394650/s3394650_142838520357353.jpg • https://st-cn.meishij.net/r/23/225/2118773/s2118773_142471761675876.jpg • https://st-cn.meishij.net/r/85/180/5045085/s5045085_145014288167252.jpg • https://st-cn.meishij.net/r/71/149/9599821/s9599821_150509435566915.jpg • https://st-cn.meishij.net/r/139/60/2827639/s2827639_151556829530544.jpg • https://st-cn.meishij.net/r/199/170/3917699/s3917699_142889626409737.jpg • https://st-cn.meishij.net/r/41/203/113291/s113291_154337102842238.jpg • https://st-cn.meishij.net/r/08/75/3768758/s3768758_143164448562685.jpg • https://st-cn.meishij.net/r/206/231/5120456/s5120456_147748643457600.jpg • https://st-cn.meishij.net/r/50/123/6030800/s6030800_155374584131082.jpg • https://st-cn.meishij.net/r/41/203/113291/s113291_154468650537397.jpg • https://st-cn.meishij.net/r/41/203/113291/s113291_154337576945105.jpg • https://st-cn.meishij.net/r/20/89/1272270/s1272270_142554525691812.jpg • https://st-cn.meishij.net/r/08/75/3768758/s3768758_142763265871365.jpg • https://st-cn.meishij.net/r/41/203/113291/s113291_154088128763034.jpg • https://st-cn.meishij.net/r/246/212/8615746/s8615746_150003929415096.jpg • https://st-cn.meishij.net/r/41/203/113291/s113291_154338772988443.jpg • https://st-cn.meishij.net/r/19/208/1364519/s1364519_44452.jpg • https://st-cn.meishij.net/r/41/203/113291/s113291_154338548476834.jpg • https://st-cn.meishij.net/r/97/32/4758097/s4758097_150520042704148.jpg • https://st-cn.meishij.net/r/41/203/113291/s113291_154338475806551.jpg • https://st-cn.meishij.net/r/118/144/6286118/s6286118_146857570754913.jpg • https://st-cn.meishij.net/r/95/122/8905595/s8905595_148008095338853.jpg • https://st-cn.meishij.net/r/41/203/113291/s113291_154338658073949.jpg • https://ali.xinshipu.cn/20170204/original/148619691827.jpg • https://st-cn.meishij.net/r/41/203/113291/s113291_154089314708674.jpg • https://st-cn.meishij.net/r/115/102/588115/s588115_153477246215536.jpg • https://st-cn.meishij.net/r/60/35/3321310/s3321310_154891634276312.jpg • https://st-cn.meishij.net/r/219/162/6603219/s6603219_151290376599435.jpg	自研引擎-A
• https://guangdong-5.zos.ctyun.cn/bucket-cc45/zs0101.json • https://w-1331615372.cos.ap-guangzhou.myqcloud.com/zs0101.json • https://ganggan1226.gz.bcebos.com/zs0101.json	com/westpm/hlahl/ui/activity/OpeningActivity.java
• https://www.miqt.cn/index.html	com/westpm/hlahl/ui/activity/webActivity.java
• http://192.20.10.4:8080/food	com/westpm/hlahl/util/Constant.java

第三方SDK

SDK名称	开发者	描述信息
AgentWeb	Justson	AgentWeb 是一个基于的 Android WebView ， 极度容易使用以及功能强大的库，提供了 Android WebView 一系列的问题解决方案 ， 并且轻量和极度灵活。
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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

邮箱

EMAIL	源码文件
123456789@qq.com	com/westpm/hlahl/ui/activity/OpeningActivity.java

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。