



ANDROID 静态分析报告



◆ 微米花. • v4.1.2

分析日期: 2025-04-30 13:12:19

i应用概览

文件名称:	微米花.apk
文件大小:	16.54MB
应用名称:	微米花
软件包名:	com.xvhcva.pvrsfvhd
主活动:	com.wmhha.ui.activitys.JDXF0ACT
版本号:	4.1.2
最小SDK:	22
目标SDK:	28
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	43/100 (中风险)
杀软检测:	17 个杀毒软件报毒
MD5:	08e2031062b40ad5a9e79ee5d960b8b8
SHA1:	67b22a81b4bb3321d641cb57f6c84638449d95d1
SHA256:	867ee384cc60e37a57b84de8dd11c05abbf66d4d0fc809932e95e7e7944d30a3

⚠️ 恶意软件家族信息

恶意家族	Cyanopica
描述信息	Cyanopica (灰喜鹊) 家族是南明离火平台识别出并命名的一系列仿冒金融应用的诈骗软件，专门设计来诱骗用户安装并窃取他们的个人及财务信息。这些应用通过加密技术将URL隐藏在云端（例如Imysqlcloud、阿里云OSS、亚马逊云等）中，以掩盖真实的服务器地址，从而巧妙地避开安全检测和追踪。此外，Cyanopica家族可能还实施了线路冗余策略，进一步增强了其隐蔽性和操作的复杂性，对用户的网络安全和财产安全构成了显著威胁。
C2服务器	目前只能观察到云服务器的 IP 地址，真实的 CC 服务器 IP 被隐藏。
凭证数据	升级会员: 解锁高级权限
关联情报	升级会员: 解锁高级权限

🔍 分析结果严重性

🚨 高危	⚠️ 中危	i 信息	✓ 安全	🔍 关注
5	11	2	2	4

四大组件信息

Activity组件: 42个, 其中export的有: 0个
Service组件: 1个, 其中export的有: 0个
Receiver组件: 2个, 其中export的有: 2个
Provider组件: 3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: None
主题: C=HPbazHwx, ST=ScUnZCyn, L=BDtaCjrV, O=BNsyfTfH, OU=MHXWKxRI, CN=NpWOiTx
签名算法: rsassa_pkcs1v15
有效期自: 2024-11-11 02:47:47+00:00
有效期至: 2034-11-09 02:47:47+00:00
发行人: C=HPbazHwx, ST=ScUnZCyn, L=BDtaCjrV, O=BNsyfTfH, OU=MHXWKxRI, CN=NpWOiTx
序列号: 0xef09287c0c375767
哈希算法: sha256
证书MD5: 76caea21e7296e64ef4fd4cd3501c173
证书SHA1: 23ae60f55a6d462a877c999611382ab8e9b21b67
证书SHA256: 787a8dc9eeb7246898b1cba68e6814737bf586be77c989a4b9e1d527d75521bf
证书SHA512: b9b3d49afa2bc6907e7cb60a39e6eb8b450e42ba670140b3dbcaed41c343bed6650a85b6ed3d051df0eaec46c9fd370cc2873b68cafb0096421c1a7b15e28b3

公钥算法: rsa
密钥长度: 2048
指纹: 04c7e5a1e11c7a6d5de1941036026aae9218391d8e2beeb137511e337b09e8eb
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.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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
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.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_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_CONTACTS	危险	读取联系人信息	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.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.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.WRITE_CALL_LOG	危险	写入通话记录	允许应用程序写入（但不读取）用户的通话记录数据。
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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0以上系统允许安装未知来源应用程序权限。
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。
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_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.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。

🔒 网络通信安全

序号	范围	严重级别	描述
----	----	------	----

🇨🇳 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	应用程序使用代码签名证书进行签名

🔍 MANIFEST分析

高危: 1 | 警告: 3 | 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	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	Broadcast Receiver (com.bas e.commonlibrary.netstate. NetworkStateReceiver) 未被 保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。
4	Broadcast Receiver (com.w mhha.gzd.FZGBReceiver) 未 被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。

</> 安全漏洞检测

高危: 4 | 警告: 7 | 信息: 2 | 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-9	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
3	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
4	不安全的WebView实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员: 解锁高级权限
5	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
6	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员: 解锁高级权限

7	SHA-1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
8	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
9	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
10	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-3	升级会员: 解锁高级权限
11	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员: 解锁高级权限
12	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
13	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板, 因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员: 解锁高级权限
14	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

动态库分析

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	arm64-v8a/libfacedevice.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缓冲区覆盖。这样可以防止在函数返回之前验证栈哨兵的完整性来检测溢出。	Full RELRO info 此共享对象已完全启用RELRO。RELRO确保GOT不会在易受攻击的ELF二进制文件中被覆盖。在完整RELRO中，整个GOT(.got和.got.plt两者)被标记为只读。	No info 二进制文件没有设置运行时搜索路径或RPATH	No info 二进制文件没有设置RUNPATH	True info 二进制文件有以下加固函数:['_vsprintf_chk','_memmove_chk','_strchr_chk','_memset_chk','_memcpy_chk','_strcpy_chk','_vsnprintf_chk','_strlen_chk']	True info 符号被剥离

2	arm64-v8a/libtoyger.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。	Full RELRO info 此共享对象已完全启用RELRO。RELRO确保GOT不会在易受攻击的ELF二进制文件中被覆盖。在完整RELRO中，整个GOT(.got和.got.plt两者)被标记为只读。	No ne info 二进制文件没有设置运行时搜索路径或RPATH。	No n o ne 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。
---	------------------------	---	---	---	--	--	--	---	--

❏ 行为分析

编号	行为	标签	文件
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
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
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
00091	从广播中检索数据	信息收集	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
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
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
00003	将压缩后的位图数据放入JSON对象中	相机	升级会员: 解锁高级权限
00001	初始化位图对象并将数据 (例如JPEG) 压缩为位图对象	相机	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
00002	打开相机并拍照	相机	升级会员：解锁高级权限
00183	获取当前相机参数并更改设置	相机	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
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
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
00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限
00023	从当前应用程序启动另一个应用程序	反射 控制	升级会员：解锁高级权限
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	升级会员：解锁高级权限
00130	获取当前WiFi信息	WiFi 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
00082	获取当前WiFi MAC地址	信息收集 WiFi	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	9/30	android.permission.READ_PHONE_STATE android.permission.WRITE_CONTACTS android.permission.READ_CONTACTS android.permission.READ_SMS android.permission.CAMERA android.permission.WRITE_CALL_LOG android.permission.READ_CALL_LOG android.permission.RECORD_AUDIO android.permission.REQUEST_INSTALL_PACKAGES

其它常用权限	10/46	android.permission.INTERNET android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.CHANGE_NETWORK_STATE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.READ_MEDIA_AUDIO
--------	-------	--

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
nice800.com	安全	是	IP地址: 43.132.110.135 国家: 中国 地区: 香港 城市: 香港 纬度: 22.285521 经度: 114.157692 查看: 高德地图
appxvcfrqweqwa-1326638684.cos.ap-guangzhou.myqcloud.com	安全	是	IP地址: 27.155.119.189 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
ijljkjzxcv-1324028813.cos.ap-guangzhou.myqcloud.com	安全	是	IP地址: 27.155.119.189 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
h5.dafsdfdfuy.cn	安全	否	No Geolocation information available.
www.beizhuabao.com	安全	否	No Geolocation information available.
jzlwjfanjzxcv.s3.ap-east-1.amazonaws.com	安全	是	IP地址: 3.5.238.134 国家: 中国 地区: 香港 城市: 香港 纬度: 22.285521 经度: 114.157692 查看: 高德地图

URL链接分析

URL信息	源码文件
-------	------

- http://h5.dafsdfdfuy.cn:9005/ - https://android-donwload.oss-cn-hangzhou.aliyuncs.com/domai0dsfnname/5100sdfh0635.text/	com/wmhha/mjyp/BuildConfig.java
https://nice800.com	com/wmhha/ui/activitys/MT7ACT.java
http://www.beizhuabao.com	com/wmhha/mjyp/app/api/Api.java
http://www.beizhuabao.com	com/wmhha/mjyp/app/api/Api2.java
- https://appxvcfrweqwa-1326638684.cos.ap-guangzhou.myqcloud.com - https://jzlwjfanjzxcv.s3.ap-east-1.amazonaws.com - https://ijljkjzxcv-1324028813.cos.ap-guangzhou.myqcloud.com	com/wmhha/mjyp/app/api/ApiQsUtil.java
https://nice800.com/	com/wmhha/ui/activitys/MT10ACT.java
https://render.alipay.com/p/yuyan/180020010001208736/alipayfacewelcome.html	自研引擎 JS

第三方SDK

SDK名称	开发者	描述信息
金融级真人认证 SDK	Alibaba	金融级真人认证服务搭载真人检测和人脸比对等生物识别技术，配合权威数据源验证，可快速校验自然人的真实身份。
C++ 共享库	Android	在 Android 应用中运行原生代码。
AgentWeb	Justson	AgentWeb 是一个基于的 Android WebView，极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 and 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。

密钥凭证

可能的密钥
凭证信息=> "com.amap.com.wmhha.mjyp.app.api.v2.apikex": "0bsdfvdd0"
f4qgkb85q4pMRMChLeC7uSn2wwTWGXrs
ae7315f546bb02c65fa5ebbf03
0a4b79afca7c44f1ade10b93fcae9ca1
09ce2f7bfb9243debf2c2efe05a1d041
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC3DtFIIG5OhLgYu4IA3GAx4DAhLyag2HSd2lsr1L66hH9SdefhaknsujWnumk+yNMYIQFdDnJ1Z8A4kj6zLJYRnNLyUeU0tI9uHPr6AGLdiaV85BoK0YXJY6pxEw3w55ooznTjMswlRyv93o8fBKWx/7mEnsrayE8VITzHroluQIDAQAB
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5HVtqOdwdaa8ISC3nfDgZaDXDi2l1zcPz9PF2Ahv2uG1ghz2uI53Lp1Y23l2KqDQtb6qw9wscvwPGvQUIWDT0oIFBQJmYc5xv9VNKEDAE5dD2CDUFH8LwoGbzeUrB7VZYx0iQQzVAgTOxBNj3879GFy3BAezm+URmnVtd3anQIDAQAB

免责声明及风险提示:

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，深入扫描软件中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成