南明离火
移动应用检测平台

ANDROID 静态分析报告

玛特宇宙 • v5.2.7

分析日期: 2024-04-01 11:39:10

应用概览

文件名称:	玛特宇宙_5.2.1.apk
文件大小:	96.37MB
应用名称:	玛特宇宙
软件包名:	com.sc.scxm
主活动:	com.sc.scxm.mvp.SplashActivity
版本号:	5.2.1
最小SDK:	21
目标SDK:	30
加固信息:	360加固 加固
应用程序安全分数:	45/100 (中风险)
杀软检测:	AI评估：可能有安全隐患
MD5:	aa1de8c05d76be3f8191f9776511fa28
SHA1:	eca2befba789dc8233a3f44cebd87d3a5fa8ad21
SHA256:	626cc5fa5b823801fe5334f77d7d1901ec9744b340d58c46420f9556854b115a

分析结果严重性分布

高危	中危	信息	安全	关注
4	27	0	1	3

四大组件导出状态统计

Activity组件：365个，其中export的有：2个
Service组件：17个，其中export的有：7个
Receiver组件：15个，其中export的有：11个
Provider组件：23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

本报告由南明离火移动安全分析平台生成

v4 签名: False
主题: CN=中国
签名算法: rsassa_pkcs1v15
有效期自: 2023-11-17 02:12:44+00:00
有效期至: 2048-11-10 02:12:44+00:00
发行人: CN=中国
序列号: 0x497933b0
哈希算法: sha256
证书MD5: 37c2d906d529386b5101438a4a6e2934
证书SHA1: fddfb22c0551b486a3d1d7db834c87a5d5fc775b
证书SHA256: 36f62942949ad6b9ceb5aec0ac1121befff35058823832448a2a2882b78f93b0
证书SHA512:
eec0c045c5196a2fa5b63b1ac873830593ce653540706a3e9a802b3303452d7428ba1fdb4cb9489a706208b46a6bb2e5fb034356ae7cc324410440cc555b7418

公钥算法: rsa
密钥长度: 2048
指纹: 1a7bf226bd5de0b3edefb334ab7a8810c167d369b64b4cfb61816c2f6d03edbe
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.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_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.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.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.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_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.READ_PRIVILEGED_PHONE_STATE	未知	未知权限	来自 android 引用的未知权限。
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_MEDIA_STORAGE	签名(系统)	获取外置SD卡的写权限	允许应用程序在外置SD卡中进行写入操作。
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。
android.permission.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。

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.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.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.CHANGE_CONFIGURATION	危险	改变UI设置	允许应用程序 允许应用程序更改当前配置，例如语言区域或整体的字体大小。
android.permission.ACCESS_SUPERUSER	危险	获取超级用户权限	有root的设备声明超级用户权限。
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_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与软件可见性相关的权限，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.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.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。
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.sc.scxm.permission.MIPUSH_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
com.meizu.flyme.push.permission.RECEIVE	普通	魅族push服务权限	魅族push服务权限。
com.sc.scxm.push.permission.MESSAGE	未知	未知权限	来自 android 引用的未知权限。
com.meizu.c2dm.permission.RECEIVE	普通	魅族push服务权限	魅族push服务权限。
com.sc.scxm.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
android.permission.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
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.CHANGE_WIFI_MULTICAST_STATE	危险	允许接收WLAN多播	允许应用程序接收并非直接向您的设备发送的数据包。这样在查找附近提供的服务时很有用。这种操作所耗电量大于非多播模式。
android.permission.INSTALL_PACKAGES	签名(系统)	请求安装APP	允许应用程序安装全新的或更新的 Android 包。恶意应用程序可能会借此添加其具有任意权限的新应用程序。

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。
com.sec.android.provider.badge.permission.READ	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	普通	在应用程序上显示通知计数	在apex的应用程序启动图标上显示通知计数或徽章。
com.majeur.launcher.permission.UPDATE_BADGE	普通	在应用程序上显示通知计数	在solid的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
android.permission.READ_APP_BADGE	普通	显示应用程序通知	允许应用程序显示应用程序图标徽章。
com.oppo.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	未知权限	来自 android 引用的未知权限。
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	未知权限	来自 android 引用的未知权限。
com.meizu.flyme.permission.PUSH	未知	未知权限	来自 android 引用的未知权限。
com.sc.scxin.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
com.sc.scxin.permission.PUSH_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
com.hihonor.push.permission.READ_PUSH_NOTIFICATION_INFO	未知	未知权限	来自 android 引用的未知权限。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.sc.scxm.mvp.SplashActivity	Schemes: openapp://, Hosts: test, Ports: 8000, Paths: /detail,
com.sc.scxm.mvp.MainActivity	Schemes: 您配置的协议，也就是你定义的 scheme pushscheme://, Hosts: 您配置的 hostname com.tencent.qcloud, Paths: 您配置的 path /detail,

网络通信安全风险分析

高危: **4** | 警告: **1** | 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。
2	*	警告	基本配置配置为信任系统证书。
3	*	高危	基本配置配置为绕过证书固定。
4	*	高危	基本配置配置为信任用户安装的证书。
5	*	高危	基本配置配置为绕过证书固定。

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	应用程序已使用代码签名证书进行签名
应用程序存在Janus漏洞	警告	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

Manifest 配置安全分析

高危: **0** | 警告: **24** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 5.0-5.0.2 [minSdk=21]	警告	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	应用程序具有网络安全配置 [android:networkSecurityConfig=0x7f150004]	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。

4	Broadcast Receiver (com.xiaomi.push.service.receivers.NetworkStatusReceiver) 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。
5	Broadcast Receiver (com.xiaomi.push.service.receivers.PingReceiver) 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。
6	Broadcast Receiver (com.sc.scxm.txim.push.OEMPush.XiaomiMsgReceiver) 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。
7	Service (com.sc.scxm.txim.push.OEMPush.HUAWEIHmsMessageService) 未被保护。 存在一个intent-filter。	警告	发现 Service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Service是显式导出的。
8	Broadcast Receiver (com.sc.scxm.txim.push.OEMPush.MEIZUPushReceiver) 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。
9	Broadcast Receiver (com.sc.scxm.txim.push.OEMPush.VIVOPushMessageReceiverImpl) 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。
10	Service (com.heytap.msp.push.service.CompatibleDataMessageCallbackService) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.coloros.mcs.permission.SEND_MCS_MESSAGE [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。
11	Service (com.heytap.msp.push.service.DataMessageCallbackService) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.heytap.mcs.permission.SEND_PUSH_MESSAGE [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。
12	Service (com.sc.scxm.txim.push.OEMPush.MyHonorMessageService) 未被保护。 存在一个intent-filter。	警告	发现 Service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Service是显式导出的。
13	Broadcast Receiver (com.sc.scxm.txim.LanguageReceiver) 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。

14	Activity (com.sc.scxm.mvp.MainActivity) 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。
15	Activity (com.sc.scxm.mvp.mine.shop.BuyOrderPayMoneyActivity) 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。
16	Broadcast Receiver (com.yc.video.old.other.NetChangedReceiver) 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。
17	Broadcast Receiver (com.tencent.android.mipush.XMPushMessageReceiver) 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。
18	Broadcast Receiver (com.meizu.cloud.pushsdk.MzPushSystemReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: com.meizu.flyme.permission.PUSH [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。
19	Broadcast Receiver (com.tencent.android.mzpush.MZPushMessageReceiver) 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。
20	Broadcast Receiver (com.tencent.android.vivopush.VivoPushMessageReceiver) 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。
21	Service (com.huawei.android.hms.tpns.HWHmsMessageService) 未被保护。 存在一个intent-filter。	警告	发现 Service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Service是显式导出的。
22	Service (com.huawei.hms.support.api.push.service.HmsMsgService) 未被保护。 存在一个intent-filter。	警告	发现 Service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Service是显式导出的。
23	Service (com.tencent.android.tpush.honor.HonorMessageService) 未被保护。 存在一个intent-filter。	警告	发现 Service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Service是显式导出的。
24	数据短信接收端设置在端口: 8000 上 [android:port]	警告	一个二进制短信接收器被配置为监听一个端口。发送到设备的二进制短信由应用程序以开发者选择的方式处理。这个短信中的数据应该被应用程序正确地验证。此外，应用程序应该假设接收到的短信来自一个不可信的来源。
25	高优先级的Intent (1000) [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。

代码安全漏洞检测

序号	问题	等级	参考标准	文件位置

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)	SYMBOLSSTRIPPED(裁剪符号表)
1	arm64-v8a/libdf_liveness_api_action.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。		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。	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	False warning 符号可用

2	arm64-v8a/libdf_liveness_jni_action.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。		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。	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	False warning 符号可用
3	arm64-v8a/libPassGuard.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。		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。	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	False warning 符号可用

4	arm64-v8a/librtmp-jni.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。		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。	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	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	9/30	android.permission.READ_PHONE_STATE android.permission.WRITE_SETTINGS android.permission.MODIFY_AUDIO_SETTINGS android.permission.RECORD_AUDIO android.permission.CAMERA android.permission.VIBRATE android.permission.SYSTEM_ALERT_WINDOW android.permission.WAKE_LOCK android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	14/46	android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE android.permission.BLUETOOTH android.permission.ACCESS_SUPERUSER android.permission.CHANGE_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_AUDIO android.permission.READ_MEDIA_VIDEO android.permission.FLASHLIGHT

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
www.openssl.org	安全	否	**IP地址:** 34.36.58.177 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
store.hispace.hicloud.com	安全	是	**IP地址:** 49.4.47.241 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
appgallery.cloud.huawei.com	安全	是	**IP地址:** 49.4.35.16 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
cloud.tencent.com	安全	是	**IP地址:** 150.139.230.71 **国家:** China **地区:** Shandong **城市:** Jinan **纬度:** 36.668331 **经度:** 116.997223 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件

- https://data-drru.push.dbankcloud.com
- https://github.com/KhronosGroup/glTF/pull/874
- https://store-drru.hispace.hicloud.com/hwmarket/api/
- http://www.tonyparisi.com/
- http://mrdoob.com
- https://laozicloud-sdk.obs.myhuaweicloud.com
- http://thap.bee360.com.cn/scnft/h5_default/xxxkkk.glb
- https://data-dre.push.dbankcloud.com
- https://grs.dbankcloud.asia
- https://github.com/KhronosGroup/glTF/pull/1163
- http://erichaines.com
- https://waibu-demo.obs.cn-east-2.myhuaweicloud.com
- http://mrdoob.com/
- https://data-dra.push.dbankcloud.com
- https://grs.dbankcloud.com
- https://github.com/KhronosGroup/glTF/tree/master/extensions/2.0/Vendor/MSFT_texture_dds
- https://github.com/qiao
- https://grs.dbankcloud.eu
- https://laozicloud-sdk.obs.cn-east-2.myhuaweicloud.com
- https://store1.hispace.hicloud.com/hwmarket/api/
- http://github.com/WestLangley
- https://metrics5.data.hicloud.com
- https://data-drcn.push.dbankcloud.com
- https://github.com/KhronosGroup/glTF/blob/master/specification/2.0/README.md
- https://metrics1.data.hicloud.com
- http://alteredqualia.com/
- https://github.com/richtr
- http://thap.bee360.com.cn/scnft/product/C4D9409FF8558BFA
- https://graphics.stanford.edu/papers/envmap/envmap.pdfnvec3
- https://store2.hispace.hicloud.com/hwmarket/api/
- https://github.com/takahirox
- https://metrics-dra.dt.hicloud.com
- https://metrics2.data.hicloud.com
- https://grs.dbankcloud.cn
- https://github.com/KhronosGroup/glTF/tree/master/extensions/2.0/Khronos/KHR_materials_pbrSpecularGlossiness
- https://store3.hispace.hicloud.com/hwmarket/api/
- https://github.com/KhronosGroup/glTF/tree/master/specification/2.0
- https://www.donmccurdy.com

自研引擎分析结果

• https://appgallery.cloud.huawei.com/app/ • https://store.hispace.hicloud.com/hwmarket/api/ • https://cloud.tencent.com/document/product/269/37059#.e6.ad.a5.e9.aa.a4.e5.9b.9b.ef.bc.9a.e6.9e.84.e5.bb.ba.e9.9f.b3.e8.a7.86.e9.a2.91.e9.80.9a.e8.af.9d.e5.8a.9f.e8.83.bd • https://cloud.tencent.com/document/product/269/37059#.e6.ad.a5.e9.aa.a4.e4.b8.89.ef.bc.9a.e6.9e.84.e5.bb.ba.e6.a0.b8.e5.bf.83-fragment • https://cloud.tencent.com/document/product/269/37059#.e6.ad.a5.e9.aa.a4.e4.ba.8c.ef.bc.9a.e5.88.9b.e5.bb.ba-viewpager • https://appgallery.cloud.huawei.com • https://cloud.tencent.com/document/product/269/37059#module-.e6.ba.90.e7.a0.81.e9.9b.86.e6.88.90 • https://cloud.tencent.com/document/product/269/37059#.e6.ad.a5.e9.aa.a4.e4.b8.80.ef.bc.9a.e7.bb.84.e4.bb.b6.e7.99.bb.e5.bd.95	自研引擎分析结果
• 2.4.13.4	lib/arm64-v8a/libbc_liveness_api_action.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
岳鹰全景监控	Alibaba	岳鹰全景监控，是阿里 UC 官方出品的先进移动应用线上监控平台，为多家知名企业提供服务。
银联 SDK	银联	银联在线支付网关是中国银联联合各商业银行为持卡人提供的集成化、综合性互联网支付工具，主要支持输入卡号付款、用户登录支付、闪银支付、迷你付（IC 卡支付）等多种支付方式，为持卡人提供境内外网上购物、水电煤缴费、商旅预订等支付服务。
IJKPlayer	Bilibili	IJKPlayer 是一款基于 FFmpeg 的轻量级 Android/iOS 视频播放器，具有 API 易于集成、编译配置可裁剪、支持硬件加速解码、DanmakuFlameMaster 特效清晰、简单易用等优势。
腾讯云通信 SDK	Tencent	腾讯云通信基于 IM 底层 IM 能力开发，仅需植入 SDK 即可轻松集成聊天、会话、群组、资料管理能力，帮助您实现文字、图片、短语音、短视频等富媒体消息收发，全面满足通信需要。
360 加固	360	360 加固保是基于 360 核心加密技术，给安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包，内存抓取等威胁。
腾讯云短视频 SDK	Tencent	腾讯云点播推出了短视频一站式解决方案，覆盖了视频生成、上传、处理、分发和播放在内的各个环节，帮助用户以最快速度实现短视频应用的上线。
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
RenderScript	Android	RenderScript 是用于在 Android 上以高性能运行计算密集型任务的框架。RenderScript 主要用于数据并行计算，不过串行工作负载也可以从中受益。RenderScript 运行时可在设备上提供的多个处理器（例如将 CPU 和 GPU）间并行调度工作。这样您就能够专注于表达算法而不是调度工作。RenderScript 对于执行图像处理、计算摄影或计算机视觉的应用来说尤其有用。
腾讯云实时音视频 SDK	Tencent	实时音视频（Tencent RTC）基于腾讯多年来在网络与音视频技术上的深度积累，以多人音视频通话和低延时互动直播两大场景化方案，通过腾讯云服务向开发者开放，致力于帮助开发者快速搭建低成本、低延时、高品质的音视频互动解决方案。
移动统计分析	Umeng	U-App 作为一款专业、免费的移动统计分析产品。在日常业务中帮您解决多种数据相关问题，如数据采集与管理、业务监测、用户行为分析、App 稳定性监控及实现多种运营方案等。助力互联网企业充分挖掘用户行为数据价值，找到产品更新迭代方向，实现精细化运营，全面提升业务增长效能。

敏感凭证泄露检测

可能的密钥
vivo推送的 "com.vivo.push.app_id" : " "

vivo推送的 "com.vivo.push.api_key" : " "
荣耀推送的 "com.hihonor.push.app_id" : " "
"set_password" : "新しいパスワードを設定する"
"set_pay_password" : "请设置新的支付密码"
"nav5_real_name_authentication" : "KYC　"
"nav5_real_name_authentication" : "實名認證"
"please_authentication_information" : "認証情報"
"nav5_changing_login_password" : "修改登录密码"
"nav5_real_name_authentication" : "Kontrolita"
"nav5_pay_password" : "支付密碼"
"nav5_status_already_auth" : "検証済み"
"contact_no_such_user" : "该用户不存在"
"set_affirm_password" : "新しいパスワードを確認"
"nav5_status_already_auth" : "kontrolita"
"set_affirm_pay_password" : "請確認新的支付密碼"
"set_pay_password" : "請設定新的支付密碼"
"nav5_real_name_authentication" : "Verified"
"set_password" : "请输入新密码"
"set_affirm_password" : "請確認新的登錄密碼"
"set_pay_password" : "新しい支払いパスワードの設定"
"nav5_changing_login_password" : "修改登錄密碼"
"nav5_status_already_auth" : "Verified"
"nav5_pay_password" : "pagrąsvorto"
"private_group" : "讨论组"
"nav5_status_unAuth" : "未認證"
"nav5_status_unAuth" : "認定されていません"
"nav5_real_name_authentication" : "Verificado"
"set_password" : "請設置新的登錄密碼"
"nav5_status_already_auth" : "已認證"
"nav5_status_already_auth" : "　"
"nav5_status_already_auth" : "已认证"

"please_authentication_information" : "认证信息"
"nav5_pay_password" : "支付密码"
"set_affirm_pay_password" : "请确认新的支付密码"
"please_authentication_information" : "認證信息"
"nav5_changing_login_password" : "ログインパスワードを変更する"
"nav5_real_name_authentication" : "实名认证"
"set_affirm_password" : "请确认新的登录密码"
"nav5_pay_password" : "支払いパスワード"
"nav5_status_already_auth" : "verificado"
"nav5_real_name_authentication" : "KYC設定"
"nav5_status_unAuth" : "未认证"
"set_affirm_pay_password" : "新しい支払いパスワードの確認"

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。