MoGua

Failed.APK 分析报告

APP名称:	
包名:	Failed
域名线索:	27条
URL线索:	14条
邮箱线索:	2条
分析日期:	2022年9月26日
分析平台:	摸瓜反编译平台

文件信息

文件名: base.apk
文件大小: 106.09MB
MD5值: a0c730c770437fc7c2c871ab874eb459
SHA1值: 1e6f5508f70b5f4ed1f70088d8a1e4db92f79876
SHA256值: 663da692427798655bb88158b211307dc5c07b41c250f4861a0e4629b6911f5f

APP 信息

App名称:
包名: Failed
主活动**Activity:**
安卓版本名称: Failed
安卓版本: Failed

域名线索

域名	服务器信息
github.com	**IP:** 20.205.243.166 **所属国家:** United States of America **地区:** Washington **城市:** Redmond **纬度:** 47.682899 **经度:** -122.120903

域名	服务器信息
haochezhutuiguang.qiniudn.com	**IP:** 222.75.63.244 **所属国家:** China **地区:** Ningxia **城市:** Yinchuan **纬度:** 38.468060 **经度:** 106.273064
appcashier256.95516.com	**IP:** 117.91.185.197 **所属国家:** China **地区:** Jiangsu **城市:** Yangzhou **纬度:** 32.397221 **经度:** 119.435829
test.opensso.tencent-cloud.com	**IP:** 0.0.0.1 **所属国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000
appgallery.cloud.huawei.com	**IP:** 117.78.15.51 **所属国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.116671 **经度:** 113.250000

域名	服务器信息
cloud-test.tim.qq.com	**IP:** 175.27.38.77 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232
s.file.myqcloud.com	**IP:** 61.54.91.204 **所属国家:** China **地区:** Henan **城市:** Luoyang **纬度:** 34.683609 **经度:** 112.453613
appcashier.test.95516.com	**IP:** 42.81.147.159 **所属国家:** China **地区:** Tianjin **城市:** Tianjin **纬度:** 39.142220 **经度:** 117.176666
official.opensso.tencent-cloud.com	**IP:** 118.126.71.18 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232

域名	服务器信息
cloud.tim.qq.com	**IP:** 42.81.178.177 **所属国家:** China **地区:** Tianjin **城市:** Tianjin **纬度:** 39.142220 **经度:** 117.176666
speedtest.trtc.tencent-cloud.com	**IP:** 162.14.19.55 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232
mlvbdc.live.qcloud.com	**IP:** 183.47.97.147 **所属国家:** China **地区:** Guangdong **城市:** Huizhou **纬度:** 23.083330 **经度:** 114.400002
play.google.com	**IP:** 142.251.43.14 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514

域名	服务器信息
www.qq.com	**IP:** 175.27.8.138 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232
avc.qcloud.com	**IP:** 157.148.32.34 **所属国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.116671 **经度:** 113.250000
yun.tim.qq.com	**IP:** 120.53.96.189 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232
www.webrtc.org	**IP:** 142.251.42.238 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514

域名	服务器信息
store.hispace.hicloud.com	**IP:** 49.4.44.164 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232
www.openssl.org	**IP:** 23.78.144.53 **所属国家:** United States of America **地区:** California **城市:** San Jose **纬度:** 37.339390 **经度:** -121.894958
www.ietf.org	**IP:** 104.16.44.99 **所属国家:** United States of America **地区:** Texas **城市:** Dallas **纬度:** 32.783058 **经度:** -96.806671
upload.ffmpeg.org	**IP:** 213.36.253.119 **所属国家:** France **地区:** Ile-de-France **城市:** Paris **纬度:** 48.853409 **经度:** 2.348800

域名	服务器信息
tools.ietf.org	**IP:** 50.223.129.194 **所属国家:** United States of America **地区:** Georgia **城市:** Marietta **纬度:** 33.952599 **经度:** -84.549927
openmp.llvm.org	**IP:** 54.67.122.174 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.774929 **经度:** -122.419418
informal.opensso.tencent-cloud.com	**IP:** 0.0.0.1 **所属国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000
test.tim.qq.com	**IP:** 106.55.123.101 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232

域名	服务器信息
www.baidu.com	**IP:** 110.242.68.3 **所属国家:** China **地区:** Hebei **城市:** Baoding **纬度:** 38.851109 **经度:** 115.490280
bugs.llvm.org	**IP:** 54.67.122.174 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.774929 **经度:** -122.419418

URL线索

URL信息	Url所在文件
https://play.google.com/store/apps/details?id=	Android String Resource
https://appgallery.cloud.huawei.com	Android String Resource
https://github.com/makovkastar/FloatingActionButton	Android String Resource
https://github.com/vinc3m1	Android String Resource
https://github.com/vinc3m1/RoundedImageView	Android String Resource
https://github.com/vinc3m1/RoundedImageView.git	Android String Resource

URL信息	Url所在文件
http://haochezhutuiguang.qiniudn.com/coDownload.html	Android String Resource
https://store.hispace.hicloud.com/hwmarket/api/	Android String Resource
ftp://upload.ffmpeg.org/incoming/	lib/arm64-v8a/libijkplayer.so
https://bugs.llvm.org/.	lib/arm64-v8a/libCarplatePocketOCR.so
http://openmp.llvm.org/	lib/arm64-v8a/libCarplatePocketOCR.so
http://www.openssl.org/support/faq.html	lib/arm64-v8a/libuptsmaddon.so
https://appcashier256.95516.com/gateway/mobile/json	lib/arm64-v8a/libentryexpro.so
https://appcashier.test.95516.com/gateway/mobile/json	lib/arm64-v8a/libentryexpro.so
https://appcashier256.95516.com/app/mobile/hft	lib/arm64-v8a/libentryexpro.so
https://appcashier.test.95516.com/app/mobile/hft	lib/arm64-v8a/libentryexpro.so
https://appcashier256.95516.com/app/mobile/json	lib/arm64-v8a/libentryexpro.so
https://appcashier.test.95516.com/app/mobile/json	lib/arm64-v8a/libentryexpro.so
https://appcashier256.95516.com/app/mobile/conf	lib/arm64-v8a/libentryexpro.so
https://appcashier.test.95516.com/app/mobile/conf	lib/arm64-v8a/libentryexpro.so

URL信息	Url所在文件
http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor-00	lib/arm64-v8a/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time	lib/arm64-v8a/libjingle_peerconnection_so.so
http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01	lib/arm64-v8a/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrext/playout-delay	lib/arm64-v8a/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrext/video-content-type	lib/arm64-v8a/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrext/video-timing	lib/arm64-v8a/libjingle_peerconnection_so.so
http://tools.ietf.org/html/draft-ietf-avtext-framemarking-07	lib/arm64-v8a/libjingle_peerconnection_so.so
www.baidu.com	lib/arm64-v8a/libjingle_peerconnection_so.so
https://www.openssl.org/docs/faq.html	lib/arm64-v8a/libsqlcipher.so
https://avc.qcloud.com/log/appsign.php	lib/arm64-v8a/libliteavsdk.so
https://avc.qcloud.com/log/report.php	lib/arm64-v8a/libliteavsdk.so
http://mlvbdc.live.qcloud.com/	lib/arm64-v8a/libliteavsdk.so

URL信息	Url所在文件
https://yun.tim.qq.com	lib/arm64-v8a/libliteavsdk.so
https://test.tim.qq.com	lib/arm64-v8a/libliteavsdk.so
https://cloud.tim.qq.com/v3/liveinterface/	lib/arm64-v8a/libliteavsdk.so
https://cloud-test.tim.qq.com/v3/liveinterface/	lib/arm64-v8a/libliteavsdk.so
https://test.opensso.tencent-cloud.com/v4/openim/jsonvideoinfo? sdkappid=%d&identifier=%s&usersig=%s&random=99999999&contenttype=json	lib/arm64-v8a/libliteavsdk.so
https://informal.opensso.tencent-cloud.com/v4/openim/jsonvideoinfo? sdkappid=%d&identifier=%s&usersig=%s&random=99999999&contenttype=json	lib/arm64-v8a/libliteavsdk.so
https://official.opensso.tencent-cloud.com/v4/openim/jsonvideoinfo? sdkappid=%d&identifier=%s&usersig=%s&random=99999999&contenttype=json	lib/arm64-v8a/libliteavsdk.so
www.qq.com	lib/arm64-v8a/libliteavsdk.so
https://speedtest.trtc.tencent-cloud.com	lib/arm64-v8a/libliteavsdk.so
http://obfjaaaafhiehjjf/ohae.oiaa	lib/arm64-v8a/libliteavsdk.so
http://www.openssl.org/support/faq.html	lib/arm64-v8a/libtxffmpeg.so
http://www.openssl.org/support/faq.html	lib/arm64-v8a/libuptsmaddonmi.so
https://bugs.llvm.org/.	lib/arm64-v8a/libPocketOCR.so
http://openmp.llvm.org/	lib/arm64-v8a/libPocketOCR.so

URL信息	Url所在文件
http://www.openssl.org/support/faq.html	lib/arm64-v8a/libijkffmpeg.so

邮箱线索

邮箱地址	所在文件
ffmpeg-devel@ffmpeg.org	lib/arm64-v8a/libijkplayer.so
apex@com.android mediaprovidergoogle@mediaprovidergoogle.apk featureframework@featureframework.apk framework@boot.art framework@settings.jar	lib/arm64-v8a/libmsec.so

手机线索

手机号	所在文件
18850551910	Android String Resource
17350881412	Android String Resource
19497583435	Android String Resource

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 2 unique certificates
Subject: C=China, ST=guangdong, L=shenzhen, O=中国平安财产保险股份有限公司, OU=中国平安财产保险股份有限公司, CN=中国平安财产保险股份有限公司
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-03-11 01:59:37+00:00
Valid To: 2046-03-05 01:59:37+00:00
Issuer: C=China, ST=guangdong, L=shenzhen, O=中国平安财产保险股份有限公司, OU=中国平安财产保险股份有限公司, CN=中国平安财产保险股份有限公司
Serial Number: 0x4f43b32d
Hash Algorithm: sha256
md5: a99a5d9ade00d746d271df8ae9ee6154
sha1: d5872d06034ecc5c26d2fbf22f4ac9b90d8a2db5
sha256: a90a0ac945695d0768f0b682f904a066cbade7011cec19e1d1ca1dbefe1e435c
sha512: 35ff74fe3a7b0cde5249b64d5ec17fcf8f20d962b41b20252ef883599321c5c683c008798e63ddee3b74c6b52e7b285dfc83204d829d90df6ef7e492c86b53ad
Subject: C=US, O=Android, CN=Android Debug
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-05-26 03:00:57+00:00
Valid To: 2044-05-18 03:00:57+00:00
Issuer: C=US, O=Android, CN=Android Debug
Serial Number: 0x635c84c1
Hash Algorithm: sha256
md5: 9048a47f512a141c8e7334aeabe161f6
sha1: b6b5fa6898bf482880c5b8dde14f39053b178faf
sha256: 5267f433949b457764b105a16f9018a0ea26438663f8e1df68e2e5821a00e0b0
sha512: 3ea4b76f8752587aaf30f29d80339da296f3251305aa6bd6c5d59e719f13c1034a7d9f4adc1e88b2b7e6601fa54bf4ad72ac0f0c651e19c010c57bef088d4917
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 2a7a188f68dbc504b3c6f715f3c5a9b18c190b84648d1f0d0bca31b2cd331799
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 04609cf75a06951d4edfb74b176871b4ecc892aad2c9c8b2d58e7e79796a3fbe

硬编码敏感信息

可能的敏感信息
"CPU_POWER_MODE_KEY" : "CPU_POWER_MODE_KEY"
"CPU_THREAD_NUM_KEY" : "CPU_THREAD_NUM_KEY"
"IMAGE_PATH_KEY" : "IMAGE_PATH_KEY"
"INPUT_COLOR_FORMAT_KEY" : "INPUT_COLOR_FORMAT_KEY"
"INPUT_SHAPE_KEY" : "INPUT_SHAPE_KEY"
"MODEL_PATH_KEY" : "MODEL_PATH_KEY"
"__pamina_auth_allow" : "同意授权"
"__pamina_auth_deny" : "暂不授权"
"__pamina_auth_dialog_mina_name" : "%s 申请"
"__pamina_auth_dialog_user_protocol" : "《平安小程序用户及平安服务协议》"
"__pamina_auth_login" : "授权登录"
"act_face_detect_net_token_invaild" : "操作时间太长,请退出重试开始检测"
"gejin_auth_agreement_0" : "《用户授权协议》(以下简称“本协议”)是中国平安财产保险股份有限公司（以下简称“平安”）与用户（以下简称“您”）所订立的有效合约。您通过平安好车主点击确认授权，即表示您与平安达成用户授权协议并同意接受本协议的全部约定内容。 在接受本协议之前，请您仔细阅读本协议的全部内容（特别是以下划线标注的内容）。如您不同意本协议的内容，或无法准确理解本协议任何条款的含义，请不要进行确认及后续操作。如果您对本协议有疑问的，请通过平安客服渠道进行询问，其将向您解释。"

可能的敏感信息
"gejin_auth_agreement_1" : "1. 为了便于您使用第三方服务，您同意平安将您的好车主用户ID、一账通账号、头像、昵称、登录手机号、姓名、证件类型、证件号码、性别、出生日期信息传递给平安集团。页面提示上会展示具体授权对象以及授权信息类型，点击确认授权后，授权字段通过加密通道传递给平安集团，再由平安集团通过加密通道传递至第三方。平安会要求平安集团依法使用您的上述信息，并对您的个人信息保密。"
"gejin_auth_agreement_2" : "2. 本条款所称“平安集团”是指中国平安保险（集团）股份有限公司及其直接或间接控股的公司，中国平安保险（集团）股份有限公司直接或间接作为其单一最大股东的公司，以及中国平安保险（集团）股份有限公司以其他方式直接或间接控制或有重大影响的主体。"
"gejin_auth_agreement_3" : "3. 平安是中立平台的提供者，上述第三方服务由该第三方独立运营并独立承担全部责任。因该第三方服务或其使用您的信息而产生的纠纷，或第三方服务违反相关法律法规或本协议约定，或您在使用第三方服务过程中遭受损失的，请您和第三方协商解决。"
"gejin_auth_agreement_4" : "4. 平安有权对本协议内容进行变更，并在平安网站或客户端公告的方式予以公布，该等变更自公告载明的生效时间开始生效。若您无法同意变更修改后的协议内容，您有权停止使用相关服务。"
"gejin_auth_agreement_5" : "5. 本协议之效力、解释、变更、执行与争议解决均适用中华人民共和国法律。双方在履行本协议的过程中，如发生争议，应协商解决。协商不成的，任何一方均可向平安所在地有管辖权的人民法院提起诉讼。"
"hcz_app_key_suffix" : "KuDC#T$Tdq47rJlv"
"library_FloatingActionButton_author" : "Oleksandr Melnykov"
"library_FloatingActionButton_authorWebsite" : "https://github.com/makovkastar/FloatingActionButton"
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"relief_credentials" : "身份证号"
"rym_auth_dialog_mina_name" : "%s 申请"
"rym_login_sdk_account_pwd_login" : "账号密码登录"

可能的敏感信息
"rym_login_sdk_auth_agree_link" : "《平安一账通统一账户服务协议》"
"rym_login_sdk_auth_agree_tips" : "点击授权登录即表示同意"
"rym_login_sdk_auth_bottom_tips" : "授权后平安集团将获得以下权限："
"rym_login_sdk_auth_bottom_tips2" : "· 获得您的一账通用户信息（手机号、身份信息等）"
"rym_login_sdk_auth_login_title" : "授权平安一账通%1$s账号 登录以下应用"
"rym_login_sdk_auth_title" : "登录授权"
"username" : "姓名:"
"warning_dialog_auth_failed_tips" : "初始化失败（101）"
"warning_dialog_auth_illegal_tips" : "SDK授权无效（102）"
"warning_dialog_token_invaild_tips" : "初始化失败（104）"
"warning_dialog_token_time_out" : "token超时（105）"
"zn_live_changekey" : "换个关键字试试吧~"
"zn_live_key_search" : "请输入关键字"

第三方SDK

此APP的危险动作

应用内通信
