南明离火
移动应用检测平台

ANDROID 静态分析报告

[redacted] v1.0

分析日期: 2025-07-06 22:41:16

应用概览

文件名称:	■■■■■ v1.0.apk
文件大小:	14.2MB
应用名称:	■■■■■
软件包名:	com.my.newprojectbuf
主活动:	.MainActivity
版本号:	1.0
最小SDK:	21
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:	61/100 (低风险)
杀软检测:	12 个杀毒软件报毒
MD5:	1cdf79b3ca01f02315ffe2a0103ab9b6
SHA1:	2a529b1aaa0cf200d8d0d01519ea46ca0414824
SHA256:	21ac6719b028e8 e7ea7311db3707e0432602ab60d4b8c3974932c01906

分析结果严重性分布

高危	中危	信息	安全	关注
0	5	1	1	0

四大组件导出状态统计

Activity组件：9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：0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=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f64070358103a6fea303977272d1795870d89b7711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
共检测到 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.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_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。

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**

本报告由南明离火移动安全分析平台生成

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。

代码安全漏洞检测

高危: **0** | 警告: **2** | 信息: **1** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	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
3	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
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
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
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
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
00013	读取文件并将其放入流中	文件	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

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	3/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE

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。

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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 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。

敏感凭证泄露检测

可能的密钥
HDowTFQ8MG[illegible]xKFkYOiQjX1khPSlD
JTgnVBg[illegible]NTZdGL7U28y40bXGl9nV[illegible]fbTU6sy41bXGlw==
NDoiX1c8MGhdXSc5L15LPDs[illegible]QFQJyfQ0AA392FBgZfmwaBgdqfQ==
fLXGudnV+6etqLTU/MY40bXGkNnV5W4=
PSAyXUtve2lLUSc2EwLMCcyQko0MyMDXzo7IUFdNCQvXhY2OysCTmV7JAJLOiY0VBVkZn5JCns1Nl1LJTsyA1s6OWlCFzw3KUMdZxJ3HQhlZ3MYDmdmaEpRM2V2HQhmYXMbCmd6IUReajUqWQU4MSJEWXMgKUZdO2kgGAk3ZidLD3gydUgKeGAgSwt4bCUZWXhlIB1eZGF3Swg3ZHE=
HDoiSEAaTlXhc7M0NcJhE+Tl0lIC9CVg==
GTshSl0ndCdBSjA1IlQYJyEoQ1E7Mw==

EzUvQV0xdDJCGCcxMl9RMCIjDV48OCMNVDw6LRcY
FjsoWV07IGtpUSYkKV5RIT0pQwJ1MilfVXgwJ1lZbnQoTFUwaWROUDQgGURcd1lMIDI=
FjsoWV07IGtpUSYkKV5RIT0pQwJ1MilfVXgwJ1lZbnQoTFUwaWRJVzYhK0hWIXZ9DV48OCNDWTgxew8=
YmJ2FQhibHQeCW8VB2gJMwIEHGt4MyQebWw+AkF+LT4QfGw2BSpDSm0Xf1p5Mg==
Fjs2VNnVzqetiHW1xrjZ1einrZa01P7MuMC1xobZ1cGnrYS01OjMuO0=
fHSnrbi01P3MuMG1xpfZ1dCnrYW01PcNEA==
NjsrA1k7MDRCUTF6Nl9XIz0iSEomeiJCTzs4KUxcJnoiQlsgOSNDTCY=
PSAyXUtve2lMSDx6MkhUMDM0TFV7OzRKFzc7Mg==
tNTSzLjjtca42dXEp62CdbXHqRi01NrMuPq1xpvZ1eynraa01OrMuMS1xqfZ1e6nrY+01NLMuPi1xoLZ1dCnrYK0NPMuP61xrPZ1d6nrYI=
HDoySEo7MTIN2dXVp62DtNTrzLjFtcaX2dXSp624tNT8zLjEtcaB2dXsp625tNT6zLjRtcaX2dXsp62hNTczLjttcaA
HDowTFQ8MGZBUSYgZkJIMCYnWVE6Okw=
GTshSl0ndCFCTHU/L0FUMDBoDWowJzJMSiE9KEoW
HDowTFQ8MGZMSjwgLkBdIT0lTFR1OzZISjQgL0JWXw==
BiA0RFYyHShJXS0bM1l3MxYpWFYxJwNVWzAkMkRXOw==
YmN1GghkZHAVAG8VB2h3Bjw3SnYnIgRKdhYBFX9dHgcRQmAGPl05Th8sdU5+Og==
NCQ2QVE2NTJEVzt7LF5XO29mTlA0JjVITGghMksVbQ==
fHRmzLjEtcaA2dX7p62AtNTCzLjotcacGHV8
tNTfzLj4tca02dX5Zsy4w7XGgNnVxKetgrTUx3y45JXGhtnV7iVCXDB0p62ptNTyMzLjvtcaa2dXKp62FtNTCzLjvtcaVGLTU08y4/rXHpg==
YmB/HQFkZHAZD28VB2sIPSMyQnE5FndCa2FsdBgIIm0OTwnNTU4CQFHE5WDA==
tNTazLjVtcaX2dXUp62DtNTSzLjvtKetobTU2sy4+rXGm9nVxKetibTU6sy41bXGlw==
PSAyXUtve2lLUScxJExLMCcyQko0MyMDXzo7IUFdNCQvXhY2OysCTmV7JAJLOiY0VBVkZn5JCns1Nl1LJTsyA1s6OWlCFzw3KUMdZxJ3HQhlZ3MeDWNnaEpRM2V2HQhmYXUyDmZ6IUReajUqWQU4MSjEWXMgKUZdO2kiTwowNyAcW3hhdklaeGBxGQF4bHQcAHhgJ0xcYjEkSwAxZXQ=
EzUvQV0xdDJCGCcxMl9RMCIjDV48OCMNVDwqLQ1PPCAuDUowJzZCViYxZk5XMTFm
NjsrA0s+MTQUCI1NEgWJzErQlx7FQV5cRoaGWN9AgsCaHoAExlhdxI=
HDowTFQ8MGZZVxshK09dJ3okQVc2P2ZCSDAmJ1lROjpM
GzExRlklJKetvLTU+8y45XGvNnV+6etqLTU/A3Z1cKnrZe01NLMuO+1xpVRMXxmbQ==
tNTCzLjotcac2dXlp62FtNT0zLjAtcaR2dXlp629tNTqzLnatca52dXlp62UtNTGzLjvtcar2dX7p62OtNT+DdnVwKetjrTU08y4xbXGlxi01cIN2dXIp62XtNTwzLjttcac2dXep62CtNTxzLjAtcaG2dTf
HDowTFQ8MGZeTCc9KEoYOiQjX1khPSlDMg==

MC0MRVoSNy9iUR8dE1dxZBovZEscOhQYWxYdcGRTJQwQbnJseiNUciU3dWBRGj0MV1wNFi50VRMuHH5xJh0oZ1QPPQ8bcTswK0wKLSYlQFwjMAFFVzQcAB9iAg5wdwolIg9ETzw3KxRLDwcPG3E4EjNPCmE9Cm5yJQ0efFEaPgMedgEVP2NCNiwJeX0mHSt7DDYXDxt1PxV0Y2wyZQtXfWAZHh0WOAMIa2kRZC1laycOPml+OwV+fk4TMD5GUyA1JXlQJhp3bkIHOyRqVRMSIQ==
NjsrA1k7MDRCUTF6I1VMMCYoTFQmIClfWTIxaElXNiErSFYhJw==
ECwlSEghPSlDGDA6JUJNOyAjX10xdDFFUTkxZl9dISYvSE48OiENXjw4Iw1UPDotFxg=
PSAyXUtve2lMSDx6MkhUMDM0TFV7OzRKFzM9KkgXNzsy
HjU2XRi01NDMuPq1xrnZ1e6nrYB1PSINEHUU
HiQnVNnVwqethLTUwsy477XGmtnV0KethbTU98y4xLXGgtnVxKetgrTU38y437XGlw==
IjUwSNnVwKethrTUwsy477XGmhi01MLMuOi1xpzZ1cWnrZe01NbMuO+1xrTZ1d6nrYI=
NjsoWV07IHwCFzE7MUNUOjUiXhclISRBUTYLIkJPOzgpTFwm
JTUhSBhkdC9JGLTU38y4xbXGnRg+NTZdGA==
ACQqQlkxdCBMUTkxIg1PPCAuDUowJzZCViYxZk5XMTFm
fLXGvNnV+aetl7TU/sy40bXGkNnV5W4=
YmNwGwtsZ3AZC28VB2oKMxwDFHUfMyJudQ0aAhtKIiA2QQg/bBd8WwEZJ2g9ZQ==
NDoiX1c8MGhEViExKFkWNDcyRFc7egFobAoXCWNsEBoS
Ymx3FQBgbHMeDW8VB2pMLDAVYWc+NSVgATc8P0B1BRsibCAzPHNYTTIldB59DA==
NjsrA1k7MDRCUTF6Nl9XIz0iSEomeitIXDw1aElXNiErSFYhJw==
tNTYzLjRtcaX2dXFp62OtNTQzLj4tca92dXup624tNTczLj5tcaV2dXKp62IFjsiSAw==
tNTfzLj0tcac2dX4p628tNT8zLjMtcaR2dXOp62CtNTIzLj+dDVISiM9JUiZ1cqlrzW01OnMuOK1xqvZ1dSnrYK01NjMuOi1xrfZ1e6nra201O0N
NDoiX1c8MGhEViExKFkWMCwyX1JTQqhldwILC3h0AR0WYX0=
PSAyXUtve2laXj44LV9fOiAuRWakJyNLQjI+KQNLICQnT1kmMWhOVw==
tNTCzLjotcac2dXFp62XtNTWzLjvdKetrrTU6cy4wbXGl9nV7C9JEHUU
dX2nrai01OvMuPq1xq3Z1e6nraO01OvMuPq1xq3Z1e5mzLjDtcaA2dXEp62CtNTHzLjktcaG2dXup62mtNTMzLjvem0c
tNTCzLjotcac2dXKp62FtNTCzLjvtcaV3bTU08y46bXGnNnV0aetlHW1xrjZ1funrY601NPMuOS1xobZ1e6nraa01MzMuO+1xrzZ1flmzLjQtcac2dX4p628tNT8zLjjtca42dX/
FjsoWV07IGt5QSUxfA1ZJSQqRFsUC9CVno7JVldIXk1WUowNSsgMlhe
fLXGqNnVxKetvLTU/My40bXGkNnV5W4=
tNTQzLj4tca92dXup625tNT3zLj+tcaXezowI8y4xLXGp9nV7qetj7TU2My46LXGqdnV7qetgLTUx8y46bXGqdnV7qetgHW1xrvZ1funray01PzMuO10L0kYfXQ==
Ez0qSBggJCpCWTF0I0NbOiEoWV0nMSINWTt0I1VbMCQyRFc7bmY=

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。