



应用信息



某应用

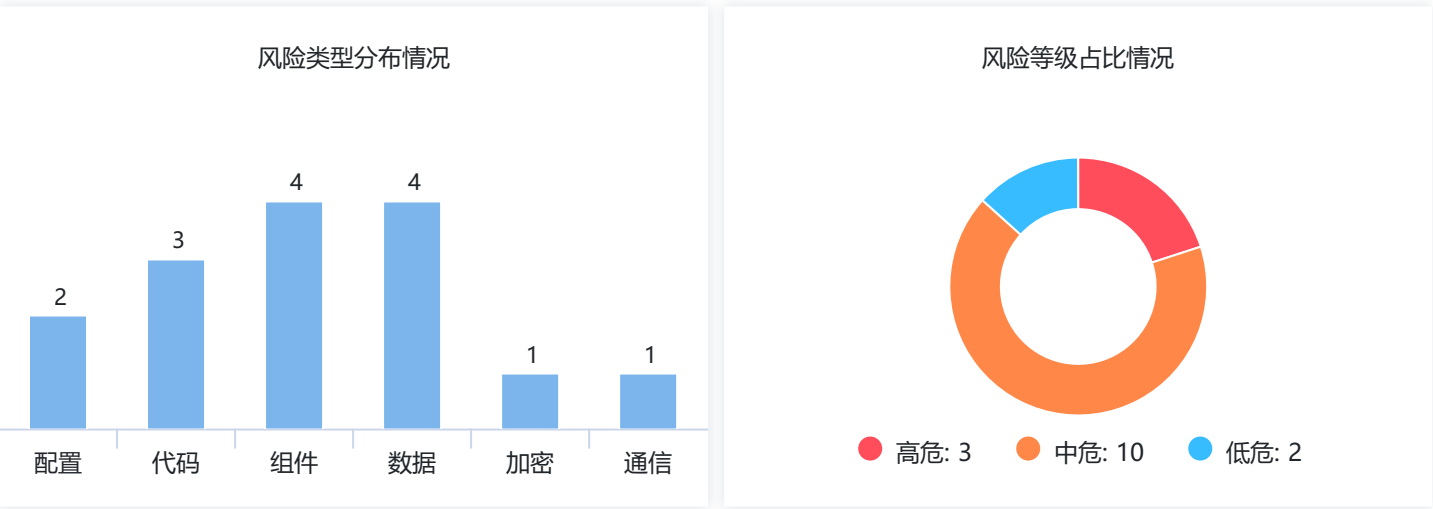
com.xxxx.xxxx.testin

应用版本:	0.59.00 (build 100)	应用类型:	Android - APK
文件大小:	11.89 MB	检测类别:	应用安全扫描
文件MD5:	5FBBC52C4328B0A3A380360442C96DD7	检测时间:	2017-10-24 19:05:10

结果概览

安全评分: 31

风险描述: 共检测 25 项, 发现 15 项风险



配置安全

—	[高危] 应用防数据备份检测	1 处风险
---	----------------	-------

风险详情: 应用程序支持备份和恢复的功能, 攻击者即可利用备份数据, 通过adb backup和adb restore在任意手机中对此应用进行数据恢复; 对于支付金融类应用, 攻击者可通过此方法来进行恶意支付、盗取存款等。

修复建议: AndroidManifest.xml配置文件中显式配置android:allowBackup=false

— [低危] 应用权限安全

5 处风险

风险详情: 应用没有严格控制权限申请, 攻击者可以通过应用获得系统权限, 例如, 访问摄像头, 麦克风录音、通讯类等, 导致用户隐私信息泄露。

修复建议: 对申请的危险权限进行严格的限制

申请权限: 检索运行的应用程序 阅读手机状态 and 身份 直接拨打电话 显示系统级警报 阅读手机状态 and 身份

代码安全

— [高危] WebView远程代码执行

4 处风险

风险详情: Android API level 16以及之前的版本存在远程代码执行安全漏洞, 该漏洞源于程序没有正确限制使用WebView.addJavascriptInterface方法, 远程攻击者可通过使用Java Reflection API利用该漏洞执行任意Java对象的方法, 简单的说就是通过addJavascriptInterface给WebView加入一个JavaScript桥接口, javascript通过调用这个接口可以直接操作本地的JAVA接口。此漏洞可能导致被安装恶意扣费软件、通讯录和短信被窃取以及被远程控制等严重后果。

修复建议: 1.建议不要使用addJavascriptInterface, 以免带来不必要的安全隐患。2.如果要使用addJavascriptInterface: 1) 如果使用HTTPS协议加载URL, 应进行证书校验防止访问的页面被篡改挂马; 2) 如果使用HTTP协议加载URL, 应进行白名单过滤、完整性校验等防止访问的页面被篡改;

风险代码: com.tencent.bugly.crashreport.CrashReport\$1.addJavascriptInterface : 1000

```
invoke-virtual (v0 p1 p2) Landroid/webkit/WebView; addJavascriptInterface ((V) Ljava/lang/Object; Ljava/lang/String;)
```

com.goluk.a6.control.browser.WebFragment.c : 143

```
invoke-virtual (v0 v1 v2) Lcom/goluk/a6/control/MyProgressWebview; addJavascriptInterface ((V) Ljava/lang/Object; Ljava/lang/String;)
```

com.handmark.pulltorefresh.library.extras.PullToRefreshWebView2.b : 90

```
invoke-virtual (v0 v1 v2) Landroid/webkit/WebView; addJavascriptInterface ((V) Ljava/lang/Object; Ljava/lang/String;)
```

umeng_bolts.k\$2.a : 164

```
invoke-virtual (v0 v1 v2) Landroid/webkit/WebView; addJavascriptInterface ((V) Ljava/lang/Object; Ljava/lang/String;)
```

— [中危] 有风险的WebView接口

4 处风险

风险详情: 使用Webview组件的addJavascriptInterface,同时没有移除 searchBoxJavaBridge_、accessibility、accessibilityTraversal 三个敏感的系统接口, 导致JS对象的远程代码执行问题

修复建议: 使用WebView.removeJavascriptInterface, 显示的移除searchBoxJavaBridge_、accessibility、accessibilityTraversal这三个危险接口

风险代码:	com.tencent.bugly.crashreport.CrashReport\$1.addJavascriptInterface : 1000 invoke-virtual (v0 p1 p2) Landroid/webkit/WebView; addJavascriptInterface ((V) Ljava/lang/Object; Ljava/lang/String;)
	com.goluk.a6.control.browser.WebFragment.c : 143 invoke-virtual (v0 v1 v2) Lcom/goluk/a6/control/MyProgressWebview; addJavascriptInterface ((V) Ljava/lang/Object; Ljava/lang/String;)
	com.handmark.pulltorefresh.library.extras.PullToRefreshWebView2.b : 90 invoke-virtual (v0 v1 v2) Landroid/webkit/WebView; addJavascriptInterface ((V) Ljava/lang/Object; Ljava/lang/String;)
	umeng_bolts.k\$2.a : 164 invoke-virtual (v0 v1 v2) Landroid/webkit/WebView; addJavascriptInterface ((V) Ljava/lang/Object; Ljava/lang/String;)

—

[低危] 本地数据库SQL注入

8 处风险

风险详情: rawQuery数据查询与execSql数据更新，是执行sql语句时不安全的处理方式，可能产生本地数据库注入的风险

修复建议: 建议不要使用不安全的方法(rawQuery/execSql)

风险代码:	com.baidu.location.c.b\$a.a invoke-virtual (v0 v2) Landroid/database/sqlite/SQLiteDatabase; execSQL ((V) Ljava/lang/String;) RiskSQL: "delete from wof where ac < " + "delete from wof where ac < "
	com.baidu.location.c.b.if invoke-virtual (v0 v2 v10) Landroid/database/sqlite/SQLiteDatabase; rawQuery ((Landroid/database/Cursor;) Ljava/lang/String; [Ljava/lang/String;) RiskSQL: "select * from wof where id = " + v0 + ";"
	com.mob.tools.utils.SQLiteHelper\$SingleTableDB.open invoke-virtual (v1 v0 v2) Landroid/database/sqlite/SQLiteDatabase; rawQuery ((Landroid/database/Cursor;) Ljava/lang/String; [Ljava/lang/String;) RiskSQL: "select count(*) from sqlite_master where type ='table' and name =' " + v1 + " "
	com.tencent.wxop.stat.au.a invoke-virtual (v1 v0) Landroid/database/sqlite/SQLiteDatabase; execSQL ((V) Ljava/lang/String;) RiskSQL: p2 + ", send_count=send_count+1 where " + v3
	com.baidu.location.c.b.if invoke-virtual (p2 v1 v2) Landroid/database/sqlite/SQLiteDatabase; rawQuery ((Landroid/database/Cursor;) Ljava/lang/String; [Ljava/lang/String;) RiskSQL: "select * from bdcltb09 where id = " + p1 + ";"
	com.baidu.location.c.b.if invoke-virtual (v0 v3 v4) Landroid/database/sqlite/SQLiteDatabase; rawQuery ((Landroid/database/Cursor;) Ljava/lang/String; [Ljava/lang/String;) RiskSQL: "select * from wof where id in (" + v4 + ");"
	com.mob.commons.logcollector.b.a invoke-virtual (v1 v3 v4) Landroid/database/sqlite/SQLiteDatabase; rawQuery ((Landroid/database/Cursor;) Ljava/lang/String; [Ljava/lang/String;)

a/lang/String; [Ljava/lang/String;)

RiskSQL: "select count(*) from " + p1

com.mob.tools.utils.SQLiteHelper.getSize

invoke-virtual (v2 v3 v4) Landroid/database/sqlite/SQLiteDatabase; rawQuery ((Landroid/database/Cursor;) Ljava/lang/String; [Ljava/lang/String;)

RiskSQL: "select count(*) from " + v4

组件安全

[中危] Activity安全-组件暴露

1 处风险

风险详情: 可导出的Activity可以被第三方APP任意调用, 被调用的 Activity 可能返回隐私的信息给恶意应用, 造成数据泄露; 攻击者也可能利用畸形数据使应用程序崩溃, 造成拒绝服务。

修复建议: 修改配置文件AndroidManifest.xml, 尽量避免Activity组件的Exported属性为true, 并且尽量不包含任何的 Intent Filter。

相关配置: 组件类型: Activity
组件名称: com.tencent.android.tpush.XGPushActivity
导出原因: android:exported=true

[中危] Broadcast安全-组件暴露

2 处风险

风险详情: Broadcast Receiver组件设置为可导出, 可能引发信息泄露、拒绝服务攻击等

修复建议: 修改配置文件AndroidManifest.xml, 尽量避免Broadcast Receivers组件的Exported属性为true。广播接收方不但需要符合 Intent filter 的接收条件, 还要求 Broadcast Receiver 也具有特定权限 (给发送方授予权限要一致) 才能接收 (双层过滤)。

相关配置: 组件类型: Broadcast Receiver
组件名称: com.tencent.android.tpush.XGPushReceiver
导出原因: intent-filter

组件类型: Broadcast Receiver
组件名称: com.goluk.a6.receiver.MessageReceiver
导出原因: android:exported=true

[中危] ContentProvider安全-组件暴露

3 处风险

风险详情: 可导出的Content Provider组件的不安全使用, 会产生SQL注入、文件遍历等漏洞, 导致用户数据泄露等。

修复建议: 修改配置文件AndroidManifest.xml, 尽量避免ContentProvider组件的Exported属性为true, 并且尽量不包含任何的 Intent Filter

相关配置: 组件类型: Content Provider
组件名称: com.umeng.facebook.FacebookContentProvider
导出原因: android:exported=true

组件类型: Content Provider
组件名称: com.tencent.android.tpush.XGPushProvider
导出原因: android:exported=true

组件类型: Content Provider
组件名称: com.tencent.mid.api.MidProvider
导出原因: android:exported=true

[中危] Service安全-组件暴露

2 处风险

风险详情: Service组件设置为可导出，存在的安全漏洞包括：权限提升，拒绝服务攻击

修复建议: 修改配置文件AndroidManifest.xml，尽量避免Service组件的Exported属性为true，并且尽量不包含任何的Intent Filter

相关配置: 组件类型: Service
组件名称: com.tencent.android.tpush.service.XGPushServiceV3
导出原因: android:exported=true

组件类型: Service
组件名称: com.tencent.android.tpush.rpc.XGRemoteService
导出原因: android:exported=true

数据安全

[高危] 内部存储文件安全

1 处风险

风险详情: Root环境中，应用在创建文件时选用MODE_WORLD_READABLE 或者MODE_WORLD_WRITEABLE模式进行权限控制，此行为存在信息泄漏的风险。

修复建议: 避免使用MODE_WORLD_WRITEABLE和MODE_WORLD_READABLE模式创建进程间通信的内部存储(Internal Storage)文件，同时避免将密码等敏感数据信息明文存储在内部存储(Internal Storage)文件中。

风险代码: com.iflytek.cloud.thirdparty.b.a
invoke-virtual (p0 v4 v5) Landroid/content/Context; openFileOutput ((Ljava/io/FileOutputStream;) Ljava/lang/String; I)
v5 = 0x1

[中危] 内网IP残留

35 处风险

风险详情: 应用的代码中，配置文件中残留开发或测试阶段使用的内网IP，可能为攻击者攻击内网服务器提供重要信息

修复建议: 移除应用代码，与配置文件中的内网IP

风险代码: com.baidu.platform.comapi.util.c.a
const-string v0 "10.0.0.200"
com.baidu.location.b.m.if
const-string v1 "10.0.0.200"
com.baidu.navisdk.util.common.NetworkUtils.fillProxy : 267
const-string v1 "10.0.0.200"
com.tencent.mid.util.Util.getHttpProxy
const-string v2 "10.0.0.200"

com.baidu.navisdk.util.common.NetworkUtils.ChangeGprsConnect : 99

const-string v1 "10.0.0.200"

com.baidu.mtjstatsdk.b.b.<clinit>

const-string v3 "10.0.0.172"

com.goluk.a6.control.AppVersionActivity.b : 54

const-string v0 "http://192.168.12.23/system/appUpgrade?xieyi=100&commid=Micle&commstag=ios&com
mdevmodel=Huawei&commappversion=1.0.0&commipcverson=CP_V1.0.1202.0493&commhdtype=CP&comm
uid=123"

com.baidu.location.b.m.if

const-string v0 "10.0.0.200"

com.baidu.location.b.m.<clinit>

const-string v0 "10.0.0.172"

com.baidu.navisdk.util.common.NetworkUtils.ChangeGprsConnect : 99

const-string v2 "10.0.0.172"

com.baidu.navisdk.util.common.NetworkUtils.PROXY_IP

PROXY_IP = "10.0.0.172"

com.baidu.platform.comapi.util.c.a

const-string v2 "10.0.0.172"

i.a

const-string v1 "10.0.0.200"

com.baidu.android.common.net.ConnectManager.checkApn

const-string v0 "10.0.0.200"

com.baidu.location.b.m.if

const-string v1 "10.0.0.172"

com.baidu.lbsapi.auth.c.a : 144

const-string v1 "10.0.0.200"

i.a

const-string v1 "10.0.0.172"

com.baidu.platform.comapi.util.c.a

const-string v0 "10.0.0.172"

com.baidu.navisdk.util.common.NetworkUtils.ChangeGprsConnect : 78

const-string v0 "10.0.0.200"

com.baidu.lbsapi.auth.f.a : 138

const-string v1 "10.0.0.172"

com.tencent.wxop.stat.common.k.a

const-string v2 "10.0.0.200"

com.baidu.mtjstatsdk.b.b.<clinit>

const-string v3 "10.0.0.200"

```
const-string v1 "10.0.0.200"
```

```
const-string v2 "10.0.0.172"
```

```
const-string v0 "10.0.0.172"
```

```
const-string v2 "10.0.0.172"
```

```
const-string v2 "10.0.0.172"
```

```
const-string v1 "10.0.0.200"
```

```
const-string v0 "10.0.0.172"
```

```
const-string v1 "10.0.0.172"
```

```
const-string v0 "10.0.0.172"
```

```
const-string v2 "10.0.0.172"
```

```
const-string v1 "10.0.0.172"
```

```
const-string v1 "10.0.0.200"
```

```
const-string v2 "10.0.0.200"
```

28 处风险

修复建议: 不要明文存放密钥在代码当中，并对APP进行加固

```
const-string v2 "000000000000000000000000000000656100000000"
```

[illegible]

```
const-string v2 "000000000000000034867844010000000000000000000000"
```

```
c = "8a3c4b262d721acd49a4bf97d5213199c86fa2b9"
```

```
const-string v2 "00000000000031381059609000000000000000000000000"
```

```
a = "a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc"
```

```
const-string v2 "0000000000000000003874204890000000000000000"
```

```
CHAT_SET = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"
```

```
const-string v1 "8a3c4b262d721acd49a4bf97d5213199c86fa2b9"
```

```
const-string v2 "000000000282429536481000000000000000000000000"
```

```
const-string v2 "0000000000000000000000000053144100000000000000"
```

```
const-string v2 "00000025418658283290000000000000000000000000000"
```

[illegible]

WX_APP_SIGNATURE = "308202eb30820254a00302010202044d36f7a4300d06092a864886f70d010105003081b9310b300906035504061302383631123010060355040813094775616e67646f6e673111300f060355040713085368656e7a68656e31353033060355040a132c54656e63656e7420546563686e6f6c6f6779285368656e7a68656e2920436f6d70616e79204c696d69746564313a3038060355040b133154656e63656e74204775616e677a686f7520526573656172636820616e6420446576656c6f706d656e742043656e7465723110300e0603550403130754656e63656e74301e170d313130313139313433933325a170d3431303131313134333933325a3081b9310b300906035504061302383631123010060355040813094775616e67646f6e673111300f060355040713085368656e7a68656e31353033060355040a132c54656e63656e7420546563686e6f6c6f6779285368656e7a68656e2920436f6d70616e79204c696d69746564313a3038060355040b133154656e63656e74204775616e677a686f7520526573656172636820616e6420446576656c6f706d656e742043656e7465723110300e0603550403130754656e63656e7430819f300d06092a864886f70d010101050003818d0030818902818100c05f34b231b083fb1323670bfbe7bdab40c0c0a6efc87ef2072a1ff0d60cc67c8edb0d0847f210bea6cbfaa241be70c86daf56be08b723c859e52428a064555d80db448cdcacc1aea2501eba06f8bad12a4fa49d85cacd7abeb68945a5cb5e061629b52e3254c373550ee4e40cb7c8ae6f7a8151ccd8df582d446f39ae0c5e930203010001300d06092a864886f70d01010500038181009c8d9d7f2f908c42081b4c764c377109a8b2c70582422125ce545842d5f520aea69550b6bd8bfd94e987b75a3077eb04ad341f481aac266e89d3864456e69fba13df018acdc168b9a19dfd7ad9d9cc6f6ace57c746515f71234df3a053e33ba93ece5cd0fc15f3e389a3f365588a9fcb439e069d3629cd7732a13fff7b891499"

```
const-string v3 "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"
```

```
const-string v2 "000000000000000000000000430467210000000000000000"
```

8/22

风险详情: 代码中残留开发或测试阶段使用的敏感URL，可能为攻击者确定攻击目标提供重要信息

修复建议: 移除应用包内的敏感的URL地址

URL列表: A = "https://at.umeng.com/iuuOHZ?cid=476"

const-string v0 "http://web.imagetest.myqcloud.com/oss/cgi_log_report"

AUTH_URL = "https://sapi.map.baidu.com/sdkcs/verify"

const-string v2 "http://p.store.qq.com/qcloudvideo?op=all"

const-string v3 "https://at.umeng.com/CCiOHv?cid=476"

am = "http://loc.map.baidu.com/offline_loc"

const-string v2 "https://www."

const-string v2 "https://mobile.umeng.com/images/pic/home/social/img-1.png"

const-string v2 "https://at.umeng.com/KHDGXb?cid=476"

const-string v2 "https://at.umeng.com/f8HHDi?cid=476"

const-string v1 "Powered by iFLYTEK "

const-string v2 "https://at.umeng.com/OTnqea?cid=476"

const-string v0 "https://svr.goluk.cn"

const-string v0 "https://surl2.goluk.cn"

const-string v1 "https://at.umeng.com/9D49bu?cid=476"

DEFAULT_OSS_ENDPOINT = "http://oss-cn-hangzhou.aliyuncs.com"

const-string v5 "http://weibo.cn/dpool/ttt/maps.php?xy=%s,%s&size=320x320&offset=%s"

const-string v0 "https://.facebook.com"

const-string v2 "https://open.weibo.cn/oauth2/authorize?"

const-string v0 "http://loc.map.baidu.com/offline_loc"

G = "https://at.umeng.com/ya4Dmy?cid=476"

B = "https://at.umeng.com/9D49bu?cid=476"

const-string v1 "https://api.weibo.com/2/proxy/darwin/graph/game/"

const-string v2 "https://at.umeng.com/KfWLzu?cid=476"

const-string v2 "https://at.umeng.com/9XXbCm?cid=476"

const-string v2 "https://at.umeng.com/WT95za?cid=476"

UPLOAD_LOG_URL = "http://client.map.baidu.com/imap/ulog/upc"

const-string v1 "http://dev.voicecloud.cn/msc/help.html"

const-string v0 "http://widget.weibo.com/invitation/app.php?"

const-string v2 "https://at.umeng.com/9D49bu?cid=476"

const-string v3 "https://sapi.map.baidu.com/sdkcs/verify"

b = "https://q.goluk.cn"

const-string v2 "https://at.umeng.com/9XXbCm?cid=476"

const-string v2 "ftp://ftp."

const-string v1 "http://dev.voicecloud.cn/msc/help.html"

k = "https://www.googleapis.com/auth/fitness.activity.read"

const-string v0 "http://android.bugly.qq.com/rqd/async"

const-string v0 "https://sapi.skyhookwireless.com/wps2/location"

const-string v2 "https://at.umeng.com/CC0LLz?cid=476"

const-string v2 "https://at.umeng.com/HL1T9j?cid=476"

const-string v1 "http://sv0.map.bdimg.com/?qt=guide&sid="

const-string v4 "http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postactlog"

h = "https://at.umeng.com/HL1T9j?cid=476"

const-string v1 "http://widget.weibo.com/relationship/followsdk.php"

const-string v0 "https://sapi.skyhookwireless.com/wps2/reverse-geo"

const-string v3 "http://app.navi.baidu.com/mobile/#navi/naing/"

const-string v2 "https://at.umeng.com/GPruqi?cid=476"

K = "https://at.umeng.com/CuKXbi?cid=476"

const-string v1 "http://yuyin.baidu.com/voice?osname=voiceopen&action=usereventflow&"

SEND_SUBMIT = "http://api.weibo.com/oauth2/sms_authorize/submit"

const-string v2 "https://at.umeng.com/1HTzyC?cid=476"

const-string v1 "http://widget.weibo.com/distribution/socail_comments_sdk.php"

COMPONENT_URL = "http://iss.openspeech.cn/v?"

const-string v4 "<LocationRQ xmlns='http://skyhookwireless.com/wps/2005' version='2.24' street-address-lookup='full'> <authentication version='2.2'> <key key='"

```
const-string v1 "http://c.data.mob.com/cdata"
```

```
FRIENDSHIPS_SHOW_URL = "https://api.weibo.com/2/friendships/show.json"
```

```
g = "https://surl3.goluk.cn"
```

```
d = "https://www.googleapis.com/auth/plus.moments.write"
```

```
const-string v3 "http://scs.openspeech.cn/scs"
```

```
const-string v1 "{\"status\":\"200\",\"expire_at\":\"86400\",\"update\":\"1466077916207\",\"zonelist_update\":\"20151129\",\"request\":\"sms_toggle\":\"1\",\"sms_home\":\"1\",\"sms_sp_region\":\"1\",\"sms_foreign\":\"1\",\"result\":{\"urls\":[{\"name\":\"sendTextSMS\",\"url\":\"http://code.sms.mob.com/verify/code\",\"params\":[\"appkey\",\"duid\",\"zone\",\"phone\",\"simserial\",\"my_phone\"],\"params_chunk\":\"\",\"encode\":\"RSA\",\"zip\":\"0\",\"request\":\"1\",\"frequency\":\"\"},{\"name\":\"submitUser\",\"url\":\"http://sdkapi.sms.mob.com/app/submituserinfo\",\"params\":[],\"params_chunk\":\"user_info_001\",\"encode\":\"RSA\",\"zip\":\"0\",\"request\":\"1\",\"frequency\":\"\"},{\"name\":\"logCollect\",\"url\":\"http://log.sms.mob.com/log/collect\",\"params\":[],\"params_chunk\":\"collect_001\",\"encode\":\"AES\",\"zip\":\"1\",\"request\":\"1\",\"frequency\":\"1:2:m\"},{\"name\":\"verifyCode\",\"url\":\"http://code.sms.mob.com/client/verification\",\"params\":[\"zone\",\"phone\",\"code\",\"appkey\",\"duid\"],\"params_chunk\":\"\",\"encode\":\"RSA\",\"zip\":\"0\",\"request\":\"1\",\"frequency\":\"\"},{\"name\":\"sendVoiceSMS\",\"url\":\"http://code.sms.mob.com/voice/verify/code\",\"params\":[\"zone\",\"phone\",\"appkey\",\"duid\"],\"params_chunk\":\"\",\"encode\":\"RSA\",\"zip\":\"0\",\"request\":\"1\",\"frequency\":\"\"},{\"name\":\"getFriend\",\"url\":\"http://addrlist.sms.mob.com/relat/fm\",\"params\":[\"appkey\",\"duid\",\"contact_phones\",\"plat\",\"sdkver\"],\"params_chunk\":\"\",\"encode\":\"RSA\",\"zip\":\"1\",\"request\":\"1\",\"frequency\":\"\"},{\"name\":\"uploadContacts\",\"url\":\"http://addrlist.sms.mob.com/relat/apply\",\"params\":[],\"params_chunk\":\"contacts_002\",\"encode\":\"RSA\",\"zip\":\"1\",\"request\":\"1\",\"frequency\":\"\"},{\"name\":\"getZonelist\",\"url\":\"http://sdkapi.sms.mob.com/utils/zonelist\",\"params\":[\"plat\",\"sdkver\",\"token\",\"appkey\",\"duid\"],\"params_chunk\":\"\",\"encode\":\"RSA\",\"zip\":\"0\",\"request\":\"1\",\"frequency\":\"\"},{\"name\":\"logInstall\",\"url\":\"http://log.sms.mob.com/log/install\",\"params\":[],\"params_chunk\":\"install_002\",\"encode\":\"AES\",\"zip\":\"1\",\"request\":\"1\",\"frequency\":\"\"},{\"name\":\"getToken\",\"url\":\"http://sdkapi.sms.mob.com/token/get\",\"params\":[\"appkey\",\"duid\",\"sdkver\",\"plat\",\"aesKey\",\"sign\"],\"params_chunk\":\"\",\"encode\":\"RSA\",\"zip\":\"0\",\"request\":\"1\",\"frequency\":\"\"}}}}"
```

```
J = "https://graph.%s"
```

```
s = "https://at.umeng.com/9XXbCm?cid=476"
```

```
const-string v0 "http://api.map.baidu.com/geosearch/v2/detail/"
```

```
const-string v0 "http://loc.map.baidu.com/iofd.php"
```

```
m = "https://www.googleapis.com/auth/fitness.location.read"
```

```
const-string v3 "http://service.weibo.com/share/mobilesdk_uappic.php"
```

```
const-string v3 "http://m.data.mob.com/cconf"
```

```
const-string v2 "ftp://anonymous:anonymous@"
```

```
f = "https://surl.goluk.cn"
```

```
j = "https://isurl.goluk.cn"
```

```
const-string v1 "http://sv0.map.bdimq.com/?qt=poi&uid="
```

```
e = "https://iserver.goluk.cn"
```

```
const-string v0 "http://loc.map.baidu.com/statloc"
```

mFeedBackURL = "http://navi.map.baidu.com/npb/"

a = "https://s.goluk.cn"

const-string v2 "https://at.umeng.com/Pn0TTr?cid=476"

o = "https://www.googleapis.com/auth/fitness.body.read"

const-string v0 "http://plus.google.com/"

const-string v0 "https://stats.umsns.com/"

const-string v2 "https://at.umeng.com/4v4XPn?cid=476"

const-string v4 "http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posterlog"

const-string v2 "http://data.openspeech.cn/index.php/clientrequest/clientcollect/isCollect"

const-string v2 "https://at.umeng.com/8Tfmei?cid=476"

e = "https://log.umsns.com/"

const-string v5 "https://www.googleapis.com/auth/games"

const-string v3 "http://daohang.map.baidu.com/mobile/#navi/naiving/start="

const-string v0 "https://api.weibo.com/oauth2/getaid.json"

const-string v0 "http://%s/%s"

const-string v0 "http://api.map.baidu.com/direction?"

const-string v0 "https://server.goluk.cn"

y = "https://at.umeng.com/9T595j?cid=476"

J = "https://at.umeng.com/LXzm8D?cid=476"

c = "https://at.umeng.com/i8Dy8n?cid=476"

const-string v1 "http://app.navi.baidu.com/distance/electroneyes?mid=2&os=android&mobile=i9300&cuid=niubi&channel=baidu&appvercode=4.0"

const-string v1 "----sdkversion:6.4.4--- 如有任何错误，请开启debug模式:在设置各平台APPID的地方添加代码：Config.DEBUG = true 所有编译问题或者设置问题，请参考文档：https://at.umeng.com/0fqeCy?cid=476"

const-string v0 "http://pingma.qq.com:80/mstat/report"

l = "https://at.umeng.com/ve4Pbm?cid=476"

p = "https://www.googleapis.com/auth/fitness.body.write"

const-string v2 "https://at.umeng.com/iWvmGD?cid=476"

const-string v3 "http://hmma.baidu.com/app.gif"

const-string v0 "https://q.goluk.cn"

const-string v2 "A ContentProvider for this app was not set up in the AndroidManifest.xml, please add %s as a provider to your AndroidManifest.xml file. See <https://developers.facebook.com/docs/sharing/android> for more info."

const-string v3 "https://sapi.map.baidu.com/sdkcs/verify"

const-string v1 "http://api.map.baidu.com/place/detail?"

const-string v2 "http://navimon.baidu.com/hunter/log/post"

f = "https://at.umeng.com/KD4zOf?cid=476"

const-string v1 "http://iss.openspeech.cn/v?"

const-string v1 "http://sv.map.baidu.com/?qt=qsdata&x="

const-string v1 "http://api.map.baidu.com/place/search?"

const-string v1 "http://api.weibo.com/oauth2/sms_authorize/send"

const-string v0 "http://loc.map.baidu.com/cc.php"

const-string v1 "https://at.umeng.com/CuKXbi?cid=476"

const-string v0 "https://facebook.com"

const-string v1 "http://sv.map.baidu.com/scape/?qt=idata&iid="

const-string v1 "https://at.umeng.com/19HTvC?cid=476"

const-string v2 "https://at.umeng.com/HL1T9j?cid=476"

n = "https://www.googleapis.com/auth/fitness.location.write"

D = "https://at.umeng.com/H5vGLj?cid=476"

const-string v1 "https://at.umeng.com/ve4Pbm?cid=476"

t = "https://at.umeng.com/GPruqi?cid=476"

const-string v1 "http://sv0.map.bdimg.com/?qt=pdata"

UPDATE_URL = "https://api.weibo.com/2/statuses/update.json"

const-string v1 "https://at.umeng.com/8Tfmei?cid=476"

const-string v2 "http://client.map.baidu.com/imap/ulog/open"

c = "https://server.goluk.cn"

URL = "http://app.navi.baidu.com/distance/electroneyes?mid=2&os=android&mobile=i9300&cuid=niubi&channel=baidu&appvercode=4.0"

const-string v5 "https://www.googleapis.com/auth/plus.me"

UPLOAD_URL = "https://api.weibo.com/2/statuses/upload.json"

```
const-string v2 "http://www."
```

```
const-string v0 "http://182.254.116.117/d?dn=99e2d153e4d0527186ebed5ac5608367&id=6&ttl=1"
```

```
d = "https://svr.goluk.cn"
```

H = "https://at.umeng.com/8Tfmei?cid=476"

```
const string v0 "http://openapi.openspeech.cn/webapi/wfr.do"
```

```
REFRESH_TOKEN_URL = "https://api.weibo.com/oauth2/access_token"
```

OAUTH2_BASE_URL = "https://open.weibo.cn/oauth2/authorize?"

```
const-string v2 "https://at.umeng.com/SLDG5z?cid=476"
```

```
const-string v0 "https://surl3.goluk.cn"
```

```
const-string v2 "https://at.umeng.com/CCOLLz?cid=476"
```

```
const-string v2 "{"status":200,"expire_at":86400,"update":1466077916207,"zonelist_update":20151129,"request":1,
"sms_toggle":1,"sms_home":1,"sms_sp_region":1,"sms_foreign":1,"result":{"urls":[{"name":"sendTextSMS","url":"
http://code.sms.mob.com/verify/code","params":["appkey","duid","zone","phone","simserial","my_phone"],"par
ams_chunk":"","encode":"RSA","zip":0,"request":1,"frequency":""},{name":"submitUser","url":"http://sdkapi.sms
mob.com/app/submituserinfo","params":[],"params_chunk":"user_info_001","encode":"RSA","zip":0,"request":1,
"frequency":""},{name":"logCollect","url":"http://log.sms.mob.com/log/collect","params":[],"params_chunk":"c
ollect_001","encode":"AES","zip":1,"request":1,"frequency":"1:2:m"},{"name":"verifyCode","url":"http://code.sms.
mob.com/client/verification","params":["zone","phone","code","appkey","duid"],"params_chunk":"","encode":"
RSA","zip":0,"request":1,"frequency":""},{name":"sendVoiceSMS","url":"http://code.sms.mob.com/voice/verify/
code","params":["zone","phone","appkey","duid"],"params_chunk":"","encode":"RSA","zip":0,"request":1,"frequ
ency":""},{name":"getFriend","url":"http://addrlist.sms.mob.com/relat/fm","params":["appkey","duid","contact
phones","plat","sdkver"],"params_chunk":"","encode":"RSA","zip":1,"request":1,"frequency":""},{name":"upload
Contacts","url":"http://addrlist.sms.mob.com/relat/apply","params":[],"params_chunk":"contacts_002","encode":
"RSA","zip":1,"request":1,"frequency":""},{name":"getZonelist","url":"http://sdkapi.sms.mob.com/utils/zonelist
","params":["plat","sdkver","token","appkey","duid"],"params_chunk":"","encode":"RSA","zip":0,"request":1,"freq
uency":""},{name":"logInstall","url":"http://log.sms.mob.com/log/install","params":[],"params_chunk":"install_0
02","encode":"AES","zip":1,"request":1,"frequency":""},{name":"getToken","url":"http://sdkapi.sms.mob.com/to
ken/get","params":["appkey","duid","sdkver","plat","aesKey","sign"],"params_chunk":"","encode":"RSA","zip":0,"
request":1,"frequency":""}}}]}
```

SINA PRIVATE URL = "http://m.weibo.cn/reg/privacyagreement?from=h5&wm=3349"

```
const-string v0 "https://isurl.goluk.cn"
```

```
const string v0 "http://api.map.baidu.com/geosearch/v2/local"
```

```
const-string v1 "http://uil.cbs.baidu.com/voiceLog/getconfig?"
```

SINA PROTOCOL URL = "http://weibo.cn/dpool/ttt/h5/regagreement.php?from=h5"

```
const-string v2 "https://at.umeng.com/KzKfWz?cid=476"
```

```
i = "https://at.umeng.com/WT95za?cid=476"
```

```
NAVI_URL = "http://app.navi.baidu.com/statistics/send"
```

const-string v0 "http://widget.weibo.com/invitation/appinfo.php?"

const-string v0 "http://service.weibo.com/share/mobilesdk.php"

PRIVACY_POLICY_WEB_URL = "http://www.goluk.cn/legal.html"

SEND_MSG = "http://api.weibo.com/oauth2/sms_authorize/send"

const-string v1 "https://at.umeng.com/LXzm8D?cid=476"

const-string v0 "http://loc.map.baidu.com/sdk.php"

j = "https://at.umeng.com/aOzmWf?cid=476"

const-string v4 "http://car.carassist.cn/uploadlog/carcontrol/"

const-string v0 "https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s"

c = "https://www.googleapis.com/auth/plus.login"

r = "https://www.googleapis.com/auth/fitness.nutrition.write"

const-string v2 "http://client.map.baidu.com/imap/ulog/upc"

const-string v0 "https://iserver.goluk.cn"

const-string v2 "https://at.umeng.com/GPruqi?cid=476"

const-string v2 ". please delete the current SDK and download the latest one. official website: <http://mta.qq.com> / or <http://mta.oa.com>"

const-string v2 "https://api.weibo.com/oauth2/access_token"

const-string v0 "https://api.weibo.com/2/proxy/sdk/statistic.json"

const-string v1 "https://api.weibo.com/2/statuses/upload.json"

const-string v1 "http://sv.map.baidu.com/scape/?qt=idata"

r = "https://at.umeng.com/9XX5ry?cid=476"

const-string v3 "http://weibo.cn/dpool/ttt/maps.php?xy=%s,%s&size=320x320&offset=%s"

i = "https://qurl.goluk.cn"

const-string v1 "http://mns.aliyuncs.com/doc/v1"

const-string v1 "https://at.umeng.com/iqmK1D?cid=476"

const-string v0 "http://loc.map.baidu.com/wloc"

q = "https://at.umeng.com/4v4XPn?cid=476"

const-string v1 "https://at.umeng.com/9T595j?cid=476"

z = "https://at.umeng.com/CCiOHv?cid=476"

const-string v2 "https://at.umeng.com/KHDGXb?cid=476"

h = "https://surl2.goluk.cn"

l = "https://at.umeng.com/19HTvC?cid=476"

j = "https://www.googleapis.com/auth/drive.appdata"

NAVI_URL_OFFLINE = "http://cq01-rdqa-pool211.cq01.baidu.com:8282/statistics/send"

F = "https://at.umeng.com/bObWzC?cid=476"

const-string v1 "http://api.weibo.com/oauth2/sms_authorize/submit"

const-string v0 "http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posteventlog"

d = "https://at.umeng.com/5P9baC?cid=476"

const-string v0 "http://loc.map.baidu.com/tcu.php"

const-string v2 "https://mobile.umeng.com/images/pic/home/social/img-1.png"

b = "https://at.umeng.com/1HTzyC?cid=476"

const-string v0 "http://api.map.baidu.com/geosearch/v2/bound"

const-string v2 "ping -c 1 -w 10 www.qq.com"

l = "https://graph-video.%s"

UPLOAD_PIC_URL = "http://service.weibo.com/share/mobilesdk_uppic.php"

WEIBO_DOWNLOAD_URL = "http://app.sina.cn/appdetail.php?applD=84560"

const-string v0 "http://loc.map.baidu.com/sdk_ep.php"

a = "https://at.umeng.com/iqmK1D?cid=476"

const-string v0 "http://192.168.12.23/system/appUpgrade?xieyi=100&commid=Micle&commstag=ios&com
mdevmodel=Huawei&commappversion=1.0.0&commipcversion=CP_V1.0.1202.0493&commhdtype=CP&comm
uid=123"

e = "https://at.umeng.com/KD4zOf?cid=476"

const-string v1 "https://api.weibo.com/2/statuses/update.json"

const-string v0 "https://qsurl.goluk.cn"

n = "https://log.umsns.com/"

const-string v0 "http://api.exc.mob.com:80"

C = "https://at.umeng.com/f8HHDi?cid=476"

const-string v0 "http://init.sms.mob.com/sdk/init"

p = "https://at.umeng.com/KHDGXb?cid=476"

p = "http://www.umeng.com/social"

const-string v2 "http://p.store.qq.com/qcloudimage?op=all"

n = "https://at.umeng.com/jiia8D?cid=476"

const-string v2 "http://p.store.qq.com/qcloudfile?op=all"

u = "https://at.umeng.com/KfWLzu?cid=476"

const-string v0 "http://pingma.qq.com:80/mstat/report"

const-string v1 "http://sv0.map.bdimg.com/?qt=guide"

const-string v2 "https://at.umeng.com/iiuOHZ?cid=476"

const-string v5 "http://m.weibo.cn/reg/privacyagreement?from=h5&wm=3349&lang="

const-string v1 "http://hxqd.openspeech.cn/launchconfig"

L = "https://at.umeng.com/0fqeCy?cid=476"

const-string v2 "https://at.umeng.com/bObWzC?cid=476"

const-string v1 "http://devs.data.mob.com:80/dsign"

const-string v0 "https://graph.%s"

const-string v0 "https://surl.goluk.cn"

const-string v1 "Powered by iFLYTEK "

const-string v1 "http://navi.map.baidu.com/npb/"

d = "A ContentProvider for this app was not set up in the AndroidManifest.xml, please add %s as a provider to your AndroidManifest.xml file. See https://developers.facebook.com/docs/sharing/android for more info."

const-string v0 "http://loc.map.baidu.com/oqur.php"

hi = "http://loc.map.baidu.com/cc.php"

const-string v2 "https://at.umeng.com/4v4XPn?cid=476"

c = "FacebookActivity is not declared in the AndroidManifest.xml, please add com.facebook.FacebookActivity to your AndroidManifest.xml file. See https://developers.facebook.com/docs/android/getting-started for more info."

const-string v1 "FacebookActivity is not declared in the AndroidManifest.xml, please add com.facebook.FacebookActivity to your AndroidManifest.xml file. See https://developers.facebook.com/docs/android/getting-started for more info."

UPLOAD_LOG_NAVI_URL = "http://navimon.baidu.com/hunter/log/post"

j = "http://log.umsns.com/link/weixin/download/"

const-string v2 "http://itsdata.map.baidu.com/long-conn-gps/sdk.php"

const-string v0 "http://api.map.baidu.com/geosearch/v2/nearby"

const-string v0 "https://sapi.map.baidu.com/sdkcs/verify"

const-string v1 "https://api.weibo.com/oauth2/getaid.json"

const-string v2 "https://at.umeng.com/iqmK1D?cid=476"

const-string v1 "http://sv0.map.bdimg.com/?qt=poi&action=1&uid="

const-string v1 "https://log.umsns.com/"

const-string v0 "http://www.baidu.com"

const-string v1 "http://dev.voicecloud.cn/msc/help.html"

w = "https://at.umeng.com/SLDG5z?cid=476"

REPOST_URL = "https://api.weibo.com/2/statuses/repost.json"

v = "https://at.umeng.com/uOjyCu?cid=476"

const-string v2 "https://at.umeng.com/19HTvC?cid=476"

const-string v0 "http://rqd.uu.qq.com/rqd/sync"

o = "https://at.umeng.com/CC0LLz?cid=476"

const-string v1 "BaiduNavi/%s (http://www.navi.baidu.com)"

const-string v1 "https://api.weibo.com/2/statuses/repost.json"

const-string v2 "https://api.weibo.com/2/friendships/show.json"

const-string v1 "https://at.umeng.com/WT95za?cid=476"

const-string v0 "http://mobile.umeng.com/images/pic/home/social/img-1.png"

const-string v0 "https://s.goluk.cn"

const-string v2 "https://at.umeng.com/jiia8D?cid=476"

const-string v2 "https://at.umeng.com/iiuOHZ?cid=476"

const-string v0 "http://api.weibo.cn/2/client/common_config"

f = "https://www.googleapis.com/auth/games"

URL = "https://sapi.map.baidu.com/sdkcs/verify"

const-string v0 "http://loc.map.baidu.com/user_err.php"

const-string v1 "语音核心技术由 科大讯飞提供 "

const-string v0 "http://lba.baidu.com/"

const-string v1 "http://app.sina.cn/appdetail.php?appID=84560"

const-string v0 "http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:specposteventlog"

k = "https://at.umeng.com/iWvmGD?cid=476"

const-string v1 "http://devs.data.mob.com:80/dinfo"

const-string v1 "Endpoint must be a string like 'http://mns.cn-****.aliyuncs.com!'"

const-string v0 "https://log.umsns.com/"

g = "https://www.googleapis.com/auth/datastoremobile"

MTA_REPORT_FULL_URL = "http://pingma.qq.com:80/mstat/report"

SHARE_URL = "http://service.weibo.com/share/mobilesdk.php"

const-string v3 "http://app.navi.baidu.com/statistics/send"

l = "https://www.googleapis.com/auth/fitness.activity.write"

const-string v2 "https://at.umeng.com/i8Dy8n?cid=476"

q = "https://www.googleapis.com/auth/fitness.nutrition.read"

const-string v1 "http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postsyslog"

const-string v2 "<ReverseGeoRQ xmlns='http://skyhookwireless.com/wps/2005' version='2.2' street-address-lookup='full'> <authentication version='2.2'> <key key=''"

g = "https://at.umeng.com/Pn0TTr?cid=476"

NAVI_URL_ONLINE = "http://app.navi.baidu.com/statistics/send"

const-string v1 "http://devs.data.mob.com:80/dinfo"

const-string v0 "http://wke.openspeech.cn/wakeup/"

const-string v1 "http://devs.data.mob.com:80/macinfo"

const-string v2 "https://at.umeng.com/OTnqea?cid=476"

const-string v0 "https://graph-video.%s"

const-string v0 "http://www.qq.com"

ALA_API_URL = "http://opendata.baidu.com"

const-string v9 "http://weibo.cn/dpool/ttt/h5/regagreement.php?from=h5&lang="

const-string v2 "https://at.umeng.com/H5vGLj?cid=476"

const-string v1 "http://mo.baidu.com/map/"

COMMENT_H5 = "http://widget.weibo.com/distribution/socail_comments_sdk.php"

const-string v2 "http://imfv.openspeech.cn/msp.do"

UPLOAD_PROTOCOL_URL = "http://client.map.baidu.com/imap/ulog/open"

const-string v1 "Endpoint must be a string like 'http://oss-cn-****.aliyuncs.com',or your cname like 'http://imag

```

e.cnamedomain.com!")

const-string v3 "https://sapi.map.baidu.com/sdkcs/verify"

i = "https://www.googleapis.com/auth/drive.file"

ad = "http://180.149.144.31:8091/offline_loc"

ATTENTION_H5 = "http://widget.weibo.com/relationship/followsdk.php"

e = "https://www.googleapis.com/auth/plus.me"

f = "http://mns.aliyuncs.com/doc/v1"

const-string v0 "http://open.weixin.qq.com/connect/sdk/qconnect?appid=%s&noncestr=%s&timestamp=%s
&scope=%s&signature=%s"

i = "http://log.umsns.com/link/qq/download/"

E = "https://at.umeng.com/KzKfWz?cid=476"

h = "https://www.googleapis.com/auth/appstate"

const-string v1 "http://mns.aliyuncs.com/doc/v1"

const-string v2 "https://at.umeng.com/ya4Dmy?cid=476"

const-string v2 "https://at.umeng.com/KD4zOf?cid=476"

m = "https://at.umeng.com/OTnqea?cid=476"

```

加密安全

— **[中危]** AES/DES弱加密 5 处风险

风险详情: 应用在使用AES/DES加密算法时，如果使用ECB（电码本）模式，攻击者将分组加密的密文进行顺序替换，对应用进行攻击，可能造成权限破解，敏感信息泄漏等问题

修复建议: 使用AES/DES加密算法时，应显式指定使用CBC（分组链接）或CFB（密码反馈）的加密模式

风险代码: **com.tencent.android.tpush.service.b.b.a : 81**
 invoke-static (v1) Ljavax/crypto/Cipher; getInstance ((Ljavax/crypto/Cipher;) Ljava/lang/String;)
 v1 = "DES/ECB/PKCS5Padding"

com.sina.weibo.sdk.utils.AesEncrypt.Decrypt : 43
 invoke-static (v2) Ljavax/crypto/Cipher; getInstance ((Ljavax/crypto/Cipher;) Ljava/lang/String;)
 v2 = "AES/ECB/PKCS5Padding"

com.sina.weibo.sdk.utils.AesEncrypt.Encrypt : 22
 invoke-static (v0) Ljavax/crypto/Cipher; getInstance ((Ljavax/crypto/Cipher;) Ljava/lang/String;)
 v0 = "AES/ECB/PKCS5Padding"

com.mob.tools.utils.Data.AES128Decode
 invoke-static (v0 v3) Ljavax/crypto/Cipher; getInstance ((Ljavax/crypto/Cipher;) Ljava/lang/String; Ljava/lang/String;)

v0 = "AES/ECB/NoPadding"

com.mob.tools.utils.Data.AES128Encode

invoke-static (v0 v3) Ljavax/crypto/Cipher; getInstance ((Ljavax/crypto/Cipher;) Ljava/lang/String; Ljava/lang/String;)

v0 = "AES/ECB/PKCS7Padding"

通信安全

—

[中危] 主机名弱校验

1 处风险

风险详情: 应用在运行过程中没有对提交数据的域名进行验证, 伪造的域名或恶意IP够窃取到应用提交的敏感数据

修复建议: 设置HostnameVerifier禁止使用ALLOW_ALL_HOSTNAME_VERIFIER, 必须使用STRICT_HOSTNAME_VERIFIER并对证书进行校验。禁止使用空的HostnameVerifier。

风险代码: **com.mob.tools.network.NetworkHelper\$3.verify**

Risk: Not verified

如您对报告内容有疑问或需其它定制化的安全检测, 请联系我们

✉ 邮箱: secconsult@testin.cn

☎ 电话: 400-900-5577