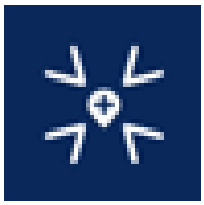
南明离火
移动应用检测平台

ANDROID 静态分析报告



宇通新能源 • v4.4.6

分析日期: 2024-05-02 20:13:12

本文仅供学习参考，如涉及侵权或其他问题，请及时联系我们进行删除或其他处理。

概述

文件名称:	com.yutong.xny_4.4.6.apk
文件大小:	24.25MB
应用名称:	宇通新能源
软件包名:	com.yutong.xny
主活动:	com.yutong.xny.activity.homepage.SplashActivity
版本号:	4.4.6
最小SDK:	19
目标SDK:	29
加固信息:	梆梆安全（企业版） 加固
MD5:	03919914d7ff2c625bfe96a862fa2b8f
SHA1:	634afaf77ac81e8eff16398f770e3d46dce3ad85
SHA256:	82de0477b4b4585a7be5896d94abea8f114e1d0a287a2555970e8d206ea13947
应用程序安全分数:	36/100 (高风险)
跟踪器检测:	7/432
杀软检测:	

分析结果严重性

高危	中危	信息	安全	关注
15	28	3	2	4

四大组件信息

Activity组件：73个，其中export的有： 3个
Service组件：20个，其中export的有： 8个
Receiver组件：9个，其中export的有： 7个
Provider组件：9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: False
主题: C=86, ST=河南, L=郑州, O=郑州宇通客车股份有限公司, OU=车联网研发中心, CN=wuhongyun
签名算法: rsassa_pkcs1v15
有效期自: 2016-09-14 00:05:39+00:00
有效期至: 2041-09-08 00:05:39+00:00
发行人: C=86, ST=河南, L=郑州, O=郑州宇通客车股份有限公司, OU=车联网研发中心, CN=wuhongyun
序列号: 0x772cd069
哈希算法: sha256
证书MD5: 29e3f226a91b218fdd47c5176a0975c3
证书SHA1: 1a83b4cab7aec18882677f1188ce2d9f17194f2a
证书SHA256: ad81f140d1124d866852206641d1a685d8fde725fa61f9e04256bf963b0fe86f
证书SHA512:
40d4b03a3b54251b88e3f3bd10fccf321839b860968e9efe38fc3cef8cc8bc87dcf81033f8c21683290dcdae86c6f7c456c6f949b1a0e16b8708f41fef77c1a4

公钥算法: rsa
密钥长度: 2048
指纹: 7c75857cce390f18d134f6e12abd5c9d1708ecb4c3cf70277e34e3325068cadd
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.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.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.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.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.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.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.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户错略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
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.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.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.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.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令，恶意应用程序可能会使用它来干扰GPS或其他位置源的操作。
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.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.BROADCAST_PACKAGE_ADDED	签名	接收新增APP的通知	它允许一个应用程序接收到其他应用程序添加新包（即新安装的可执行文件）的广播消息。
android.permission.BROADCAST_PACKAGE_CHANGED	签名	接收APP变化的通知	它允许一个应用程序接收到其他应用程序变化（安装、卸载、修改）的广播消息。
android.permission.BROADCAST_PACKAGE_INSTALL	签名	接收APP安装的通知	它允许一个应用程序接收到其他应用程序安装新包（即新安装的可执行文件）的广播消息。
android.permission.BROADCAST_PACKAGE_REPLACED	签名	接收APP替换的通知	它允许一个应用程序接收到其他应用程序被覆盖安装的广播消息。
android.permission.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
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.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
com.android.launcher.permission.READ_SETTINGS	危险	读取桌面快捷方式	这种权限的作用是允许应用读取桌面快捷方式的设置。
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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
android.permission.ACTION_MANAGE_OVERLAY_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.yutong.xny.permission.MIPUSH_RECEIVE	未知	未知权限	来自 android 引用的未知权限。

VIRUSTOTAL 扫描

扫描结果： 文件安全

网络安全配置

高危: 1 | 警告: 0 | 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。

证书分析

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

MANIFEST分析

高危: 7 | 警告: 19 | 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 4.4-4.4.4, [minSdk=19]	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=@xml/network_security_config]	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	Activity (com.yutong.xny.activity.simactivation.SIMCardActivationActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
4	Activity (com.yutong.xny.activity.simactivation.SIMCardQueryActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
5	Activity (com.yutong.xny.activity.homepage.LoginActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
6	Activity (com.yutong.xny.activity.home.HomeActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
7	Activity (com.yutong.xny.push.PushActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。

本文仅供学习参考，如涉及侵权或其他问题，请及时联系我们进行删除或其他处理。

8	Activity (com.yutong.xny.push.PushActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
9	Activity (com.yutong.xny.test.push.PushActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
10	Activity (com.yutong.xny.test.push.PushActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
11	Broadcast Receiver (com.yutong.android.push.PushBroadcastReceiver) 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。
12	Activity (com.yutong.android.push.activity.UMengNotifyActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
13	Activity (com.yutong.android.push.activity.UMengNotifyActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
14	Service (com.taobao.accs.ChannelService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
15	Service (com.taobao.accs.data.MsgDistributeService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
16	Broadcast Receiver (com.taobao.accs.EventReceiver) 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.taobao.accs.ServiceReceiver) 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	Service (org.android.agoo.accs.AgooService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
19	Service (com.umeng.message.UmengIntentService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。

20	Service (com.umeng.message.XiaomiIntentService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
21	Broadcast Receiver (com.taobao.agoo.AgooCommondReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
22	Service (com.umeng.message.UmengMessageIntentReceiverService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
23	Service (com.blankj.utilcode.util.MessengerUtils$ServerService) 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	Broadcast Receiver (org.android.agoo.huawei.HuaweiPushReceiver) 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。
25	Service (com.xiaomi.mipush.sdk.PushMessageHandler) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
26	Broadcast Receiver (com.xiaomi.push.service.receivers.NetworkStatusReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
27	Broadcast Receiver (org.android.agoo.xiaomi.MiPushBroadcastReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。

</> 源代码分析

高危: **6** | 警告: **8** | 信息: **3** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	com/yutong/android/utils/NetworkUtils.java com/yutong/basehttp/util/SunJCE.java org/android/spdy/SpdyRequest.java
				com/azhon/appupdate/utils/LogUtil.java com/baidu/b/c.java com/baidu/b/g.java com/ccolorchen/listlibrary/lib/MultiTypeAdapter.java com/ccolorchen/listlibrary/refresh/utils/LogUtils.java com/github/gzuliyujiang/dialog/DialogLog.java com/github/moduth/blockcanary/BlockCanary.java com/lzy/okgo/utils/OkLogger.java

				com/scwang/smartrefresh/layout/SmartRefreshLayout.java com/taobao/tlog/adapter/TLogConfigSwitchReceiver.java com/taobao/tlog/adapter/TLogFileUploader.java com/tbruyelle/rxpermissions2/RxPermissionsFragment.java com/yutong/android/push/PushManager.java com/yutong/android/utils/ActivityUtils.java com/yutong/android/utils/AdaptScreenUtils.java com/yutong/android/utils/AppUtils.java com/yutong/android/utils/BitUtils.java com/yutong/android/utils/CacheDiskUtils.java com/yutong/android/utils/ContactUtils.java com/yutong/android/utils/CrashUtils.java com/yutong/android/utils/FlashlightUtils.java com/yutong/android/utils/FragmentUtils.java com/yutong/android/utils/KeyboardUtils.java com/yutong/android/utils/LogUtils.java com/yutong/android/utils/NetworkUtils.java com/yutong/android/utils/ProcessUtils.java com/yutong/android/utils/SpanUtils.java com/yutong/android/utils/ThreadUtils.java com/yutong/android/utils/ToastUtils.java com/yutong/android/utils/UriUtils.java com/yutong/appmodule/bean/AppModuleBean.java com/yutong/appmodule/download/BackgroundExecutor.java com/yutong/base/utils/BackgroundExecutor.java com/yutong/base/utils/ImageUtil.java com/yutong/base/utils/SharedPreferencesUtils.java com/yutong/base/utils/TimeUtil.java com/yutong/imagepicker/ImageDataSource.java com/yutong/imagepicker/ImagePicker.java com/yutong/imagepicker/ui/ImageGridActivity.java com/yutong/jsbridge/JsApi.java com/yutong/jsbridge/WebViewActivity.java com/yutong/jsbridge/WebViewFragment.java com/yutong/jsbridge/bridge/YTWebView.java com/yutong/jsbridge/location/ContinuityMapBean.java com/yutong/jsbridge/location/MapBean.java com/yutong/mobile/android/appupdatesignhttp/widget/UpdateDialog.java com/yutong/qrcode/activity/CommonCaptureActivity.java com/yutong/shakesdk/ShakeClient.java com/yutong/shakesdk/http/HttpClient.java com/yutong/shakesdk/processor/packet/response/ConnectProcessorBase.java com/yutong/shakesdk/util/LogUtil.java com/yutong/xny/activity/alarm/CapacityActivity.java com/yutong/xny/activity/carmonitor/vehicle_mvp/map_manager/GaodeMapViewManager.java com/yutong/xny/activity/energy/EnergyDescriptionActivity.java com/yutong/xny/activity/newscenter/NewsCenterActivity.java com/yutong/xny/activity/tree/CarTreeFragment.java com/yutong/xny/activity/wirelesscharging/WirelessChargingQueryListActivity.java com/yutong/xny/utils/Logger.java com/yutong/xny/utils/pinyin/DoubleArrayTrie.java com/yutong/xny/view/charts/GridLineChartView.java com/yutong/xny/view/charts/MultiAxisChart03View.java com/yutong/xny/view/codepicker/WheelUtil.java com/yutong/xny/widget/roundprogressbar/RoundProgres
2	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-3	

				sBar.java com/yutong/xny/widget/scrollauthcode/ScrollAuthCodeView.java com/zhy/autolayout/utils/L.java me/weishu/reflection/Reflection.java me/yokeyword/fragmentation/TransactionDelegate.java me/yokeyword/fragmentation/debug/DebugStackDelegate.java me/yokeyword/fragmentation/exception/AfterSaveStateTransactionWarning.java org/android/spdy/NetTimeGaurd.java org/android/spdy/ProtectedPointerTest.java org/android/spdy/spduLog.java org/greenrobot/eventbus/Logger.java org/greenrobot/eventbus/util/ErrorDialogConfig.java org/greenrobot/eventbus/util/ErrorDialogManager.java org/greenrobot/greendao/AbstractDao.java org/greenrobot/greendao/DaoException.java org/greenrobot/greendao/DaoLog.java org/greenrobot/greendao/DbUtils.java org/greenrobot/greendao/async/AsyncOperationExecutor.java org/greenrobot/greendao/internal/LongHashMap.java org/greenrobot/greendao/query/QueryBuilder.java org/greenrobot/greendao/test/AbstractDaoTest.java org/greenrobot/greendao/test/AbstractDaoTestLongPk.java org/greenrobot/greendao/test/AbstractDaoTestSinglePk.java org/greenrobot/greendao/test/DbTest.java org/xclcharts/chart/ArcLineChart.java org/xclcharts/chart/ArcLineData.java org/xclcharts/chart/AreaChart.java org/xclcharts/chart/BarChart.java org/xclcharts/chart/BarChart3D.java org/xclcharts/chart/BubbleChart.java org/xclcharts/chart/CircleChart.java org/xclcharts/chart/DialChart.java org/xclcharts/chart/FunnelChart.java org/xclcharts/chart/GaugeChart.java org/xclcharts/chart/LineChart.java org/xclcharts/chart/PieChart.java org/xclcharts/chart/PieChart3D.java org/xclcharts/chart/RadarChart.java org/xclcharts/chart/RangeBarChart.java org/xclcharts/chart/RoseChart.java org/xclcharts/chart/ScatterChart.java org/xclcharts/chart/SplineChart.java org/xclcharts/renderer/CirChart.java org/xclcharts/renderer/EventChart.java org/xclcharts/renderer/LnChart.java org/xclcharts/renderer/RdChart.java org/xclcharts/renderer/axis/RoundAxisRender.java org/xclcharts/renderer/bar/Bar.java org/xclcharts/renderer/bar/FlatBar.java org/xclcharts/renderer/info/DyInfo.java org/xclcharts/renderer/line/PlotCustomLine.java org/xclcharts/renderer/plot/LabelBrokenLine.java org/xclcharts/view/GraphicalView.java top/zibin/luban/Checker.java top/zibin/luban/Luban.java

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	com/lzy/okgo/cache/CacheEntity.java com/lzy/okgo/exception/CacheException.java com/yutong/android/utils/constant/RegexConstants.java com/yutong/base/utils/Consts.java com/yutong/basehttp/util/DES.java com/yutong/mobile/android/MpisPush.java com/yutong/qrcode/decoding/Intents.java com/yutong/xny/BuildConfig.java com/yutong/xny/common/Constants.java com/yutong/xny/common/NetUrl.java com/yutong/xny/common/NetUrl_Overseas.java org/android/spdy/SpdyProtocol.java
4	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	com/baidu/b/c/b/b.java com/hjq/permissions/PermissionFragment.java com/yutong/android/httphelper/util/DownloadUtil.java com/yutong/android/utils/DeviceUtils.java com/yutong/mobile/android/appupdatesignhttp/utils/ColorUtils.java com/yutong/shakesdk/util/SystemUtil.java com/zhy/autolayout/widget/MetroLayout.java org/android/spdy/SpdyBytePool.java org/greenrobot/greendao/test/DbTest.java org/xclcharts/common/DrawHelper.java
5	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL注入'） OWASP Top 10: M7: Client Code Quality	com/lzy/okgo/db/DBHelper.java com/lzy/okgo/db/DBUtils.java org/greenrobot/greendao/AbstractDao.java org/greenrobot/greendao/DbUtils.java org/greenrobot/greendao/database/StandardDatabase.java
6	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/azhon/appupdate/utils/FileUtil.java com/baidu/b/d/b.java com/yutong/base/utils/EncryptUtil.java com/yutong/basehttp/Utils.java com/yutong/xny/utils/MD5Utils.java

7	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	com/baidu/b/g.java com/baidu/vi/VDeviceAPI.java com/lzy/okgo/convert/FileConvert.java com/lzy/okserver/OkDownload.java com/orhanobut/logger/CsvFormatStrategy.java com/yutong/android/httphelper/HttpUtils.java com/yutong/android/httphelper/impl/OkGoHttpProvider.java com/yutong/android/httphelper/util/DownloadUtil.java com/yutong/android/utils/CleanUtils.java com/yutong/android/utils/CrashUtils.java com/yutong/android/utils/DeviceUtils.java com/yutong/android/utils/LogUtils.java com/yutong/android/utils/PathUtils.java com/yutong/android/utils/SDCardUtils.java com/yutong/android/utils/UriUtils.java com/yutong/base/utils/SystemUtil.java com/yutong/imagepicker/ImagePicker.java com/yutong/mobile/android/appupdatesignhttp/utils/UpdateUtils.java com/yutong/shakesdk/util/SystemUtil.java com/yutong/xny/h5/photoview/PhotoViewerActivity.java
8	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	com/lzy/okgo/https/HttpsUtils.java com/yutong/android/httphelper/impl/OKGoHttpsUtils.java
9	该文件是World Writable。任何应用程序都可以写入文件	高危	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/azhon/appupdate/utils/SharePreUtil.java
10	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	com/yutong/android/utils/AppUtils.java com/yutong/android/utils/DeviceUtils.java
11	使用弱加密算法	高危	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/yutong/basehttp/Utils.java com/yutong/basehttp/util/DES.java
12	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/yutong/basehttp/Utils.java

13	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/baidu/b/d/c.java com/yutong/shakesdk/util/DeviceIdUtil.java org/repackage/a/a/a/a/c.java
14	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	com/yutong/android/utils/ClipboardUtils.java
15	不安全的Web视图实现。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	com/yutong/jsbridge/bridge/YTWebView.java
16	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-2	com/yutong/jsbridge/bridge/YTWebView.java
17	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	com/yutong/jsbridge/bridge/YTWebView.java
18	WebView域控制不严格漏洞	高危	CWE: CWE-73: 外部控制文件名或路径	com/yutong/jsbridge/bridge/YTWebView.java
19	此应用程序使用SQL Cipher。SQLCipher为sqlite数据库文件提供256位AES加密	信息	OWASP MASVS: MSTG-CRYPTO-1	org/greenrobot/greendao/database/DatabaseOpenHelper$EncryptedHelper.java

动态库分析

序号	动态库	NX(堆栈禁止执行)	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/libCHttpSign.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

2	arm64-v8a/libconceal.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/libtnet-3.1.14.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	True info 二进制文件有以下加固函数: ['__strrchr_chk', '__strlen_chk', '__sprintf_chk', '__strchr_chk', '__strcpy_chk']	False warning 符号可用

滥用权限

类型	匹配	权限

恶意软件常用权限	11/30	android.permission.REQUEST_INSTALL_PACKAGES android.permission.READ_PHONE_STATE android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.WAKE_LOCK android.permission.GET_TASKS android.permission.WRITE_SETTINGS android.permission.RECEIVE_BOOT_COMPLETED android.permission.VIBRATE android.permission.CALL_PHONE android.permission.CAMERA
其它常用权限	9/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.FLASHLIGHT android.permission.BLUETOOTH

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
mc.yutong.com	安全	是	**IP地址:** 222.85.67.167 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
eubus.vehicleplus.net	安全	否	**IP地址:** 18.65.3.88 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
mcloudtest.yutong.com	安全	是	**IP地址:** 222.85.67.167 **国家:** 中国 **地区:** 河南 **城市:** 郑州 **纬度:** 34.757778 **经度:** 113.648613 **查看:** 高德地图

cloud.yutong.com	安全	是	**IP地址:** 222.85.67.172 **国家:** 中国 **地区:** 河南 **城市:** 郑州 **纬度:** 34.757778 **经度:** 113.648613 **查看:** 高德地图
static.vehicleplus.net	安全	是	**IP地址:** 222.85.67.172 **国家:** 中国 **地区:** 河南 **城市:** 郑州 **纬度:** 34.757778 **经度:** 113.648613 **查看:** 高德地图

网址

网址信息	源码文件
• http://www.winimage.com/zLibDll	自研引擎-A
• 223.5.5.5	com/yutong/android/utils/NetworkUtils.java
• https://cloud.yutong.com/security/mpis/app/version/check/update • https://mcloudtest.yutong.com:20443/security/mpis/app/version/check/update • https://cloud.yutong.com/mpis/open_app/version/check/update • https://mcloudtest.yutong.com:20443/mpis/open_app/version/check/update	com/yutong/mobile/android/appupdate signhttp/constant/Urls.java
• https://cloud.yutong.com • https://mcloudtest.yutong.com:20443	com/yutong/shakesdk/http/api/Api.java
• https://cloud.yutong.com/barbie/app/home.do? • https://cloud.yutong.com/ • https://eubus.vehicleplus.net/ • https://static.vehicleplus.net/web/main/resource/codebase/app/xny/privacy_policy.html • https://static.vehicleplus.net/web/main/resource/codebase/app/xny/permission_usage_specification.html • https://static.vehicleplus.net/web/main/resource/codebase/app/xny/user_agreement.html	com/yutong/xny/BuildConfig.java
• https://mc.yutong.com/wxvin	com/yutong/xny/common/Constants.java
• https://eubus.vehicleplus.net/	com/yutong/xny/common/NetUrl_Overseas.java

第三方SDK

SDK名称	开发者	描述信息
梆梆安全	梆梆安全	针对目前移动应用普遍存在的破解、篡改、盗版、钓鱼欺诈、内存调试、数据窃取等各类安全风险，梆梆安全为开发者提供全面的移动应用加固加密技术和攻击防范服务。
Bugly	Tencent	腾讯 Bugly，为移动开发者提供专业的异常上报和运营统计，帮助开发者快速发现并解决异常，同时掌握产品运营动态，及时跟进用户反馈。

C++ 共享库	Android	在 Android 应用中运行原生代码。
MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高，稳定性强。
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。
AndroidUtilCode	Blankj	AndroidUtilCode 是一个强大易用的安卓工具类库，它合理地封装了安卓开发中常用的函数，具有完善的 Demo 和单元测试，利用其封装好的 APIs 可以大大提高开发效率。
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
HMS Core	Huawei	HMS Core 是华为终端云服务提供的端、云开放能力的合集，助您高效构建精品应用。
Huawei Push	Huawei	华为推送服务（HUAWEI Push Kit）是华为为开发者提供的消息推送平台，建立了从云端到终端的消息推送通道。开发者通过集成 HUAWEI Push Kit 可以实时推送消息到用户终端应用，构筑良好的用户关系，提升用户的感知度和活跃度。
HMS Update	Huawei	用于 HMS SDK 引导升级 Huawei Mobile Services(APK)，提供给系统安装器读取升级文件。
友盟推送	Umeng	基于友盟+全域数据建立精准的消息推送平台，为开发者提供更灵活、更智能、更有效的消息推送方案，有效提升用户粘性，提高 App 活跃度。
MiPush	Xiaomi	小米消息推送服务在 MIUI 上为系统级通道，并且全平台通用，可以为开发者提供稳定、可靠、高效的推送服务。
Jetpack Lifecycle	Google	生命周期感知型组件可执行操作来响应另一个组件（如 Activity 和 Fragment）的生命周期状态的变化。这些组件有助于您写出更有条理且往往更精简的代码，这样的代码更易于维护。
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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

邮箱

EMAIL	源码文件
loc-bugs@baidu.com	com/yutong/xny/utils/map/Lbs.java

追踪器

名称	类别	网址
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Baidu Map		https://reports.exodus-privacy.eu.org/trackers/99
Bugly		https://reports.exodus-privacy.eu.org/trackers/190

Huawei Mobile Services (HMS) Core	Analytics, Advertisement, Location	https://reports.exodus-privacy.eu.org/trackers/333
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
Yueying Crash SDK	Crash reporting, Analytics	https://reports.exodus-privacy.eu.org/trackers/448

🔑 密钥凭证

可能的密钥
高德地图的=> "com.amap.api.v2.apikey" : "0e8f8aede7a87a4c5bbec7d2ac0132ac"
凭证信息=> "com.google.android.geo.API_KEY" : "AIzaSyDMH4a3YvkfKXLZyFoqMArY7zFq5OlN2J4"
友盟统计的=> "UMENG_APPKEY" : "5c19d832f1f556abed0003ce"
友盟统计的=> "UMENG_CHANNEL" : "channel_name"
百度地图的=> "com.baidu.lbsapi.API_KEY" : "4mgSgfwtPw9jc51u8Mc2b5BW18l6ViHO"
华为HMS Core 应用ID的=> "com.huawei.hms.client.appid" : "appid=100107303"
1250544c49f548bf843477bc5c296928
2469dc0eb7684b479679caf84c269c25
5dd4f6710cafb2057f000457
57c9eb705e3fd08b68c0bd5b8b95091e

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。

© 2024 南明离火 - 移动安全分析平台自动生成