南明离火
移动应用检测平台

ANDROID 静态分析报告

云城计划 • v1.2.2

分析日期: 2024-05-27 15:00:46

应用概览

文件名称:	云城计划.apk
文件大小:	53.33MB
应用名称:	云城计划
软件包名:	com.yunchengjihua.app.xb9rsey
主活动:	com.lt.app.MainActivity
版本号:	1.2.2
最小SDK:	19
目标SDK:	30
加固信息:	未加壳
应用程序安全分数:	43/100 (中风险)
杀软检测:	AI评估：安全
MD5:	8343d21deb1e9587cf0dfb6ac3f4509a
SHA1:	1d533a29d76b815eafc3ca5afdfa1f68a699ddea
SHA256:	1b7820668655821b6ce317ad7514e864e778e29d43de972aff7ee7eb9bbaf7d

分析结果严重性分布

高危	中危	信息	安全	关注
5	9	2	2	0

四大组件导出状态统计

Activity组件：3个，其中export的有： 1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：2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: C=CN, CN=XCITY
签名算法: rsassa_pkcs1v15
有效期自: 2024-05-08 17:35:47+00:00
有效期至: 2049-05-09 17:35:47+00:00
发行人: C=CN, CN=XCITY
序列号: 0x594d0000000000f52cbd
哈希算法: sha256
证书MD5: 3b24128a4c95bc8b05d9be0d80a937f7
证书SHA1: b42434a4eff824c463dbf8e3a2eab04d6e7b9c4c
证书SHA256: e236ad198bb4a1d33d96653d31539227ab2339b2759d8ebd2a2f8506ad8080a5
证书SHA512:
3c85b29ed4ebf2d233dae7b7dd422ac5a2014ab5872b8d6d1ddc206baf962da723602ec4a6a566a8bfbce70459270eefd4b5e992634c28cb83b925f5cf929562

公钥算法: rsa
密钥长度: 2048
指纹: 9ea0804423c01ef10803fc4dc22fe1835a27a32d4baf7643edd69ed6a6bb25ca
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.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.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.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.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.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.yunchengjihua.app.xb9rsey.permission.MAP	未知	未知权限	来自 android 引用的未知权限。
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.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.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_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。
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。

可被览 Activity 组件分析

ACTIVITY	INTENT

com.lt.app.JumpActivity	Schemes: ltapp412337://,

网络通信安全风险分析

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

Manifest 配置安全分析

高危: **0** | 警告: **1** | 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]	信息	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/nsc]	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.lt.app.JumpActivity) 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，因此可被设备上的任何其他应用程序访问。

代码安全漏洞检测

高危: **4** | 警告: **7** | 信息: **2** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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	升级会员：解锁高级权限
2	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

3	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	升级会员：解锁高级权限
4	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
5	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
6	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
7	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
8	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	升级会员：解锁高级权限
9	WebView域控制不严格漏洞	高危	CWE: CWE-73: 外部控制文件名或路径	升级会员：解锁高级权限
10	不安全的Web视图实现。可能在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	升级会员：解锁高级权限
11	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	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

12	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	升级会员：解锁高级权限
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	升级会员：解锁高级权限
14	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	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	4/30	android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.CAMERA
其它常用权限	8/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.READ_MEDIA_AUDIO

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。

URL 链接安全分析

URL信息	源码文件
• https://t.me/LIBRA • https://eips.ethereum.org/EIPS/eip-607 • https://testnet.bscscan.com • https://eips.ethereum.org/EIPS/eip-779 • https://github.com/ethereum/eth1.0-specs/blob/master/network-upgrades/mainnet-upgrades/london.md • https://pingguatuo.qq.com/playvideo.qcloud.com • https://www.yimenapp.com/doc/echo2.cshtml • https://eips.ethereum.org/EIPS/eip-609 • http://admin888.yunchengjihua.com/uploads/20240416/be560c207816ab20a09fc79e70e6813b.png • https://www.yimenapp.com/doc/demo.cshtml	

本报告由南明离火移动安全分析平台生成

- https://cloud.tencent.com/document/product/266/45554
- https://eips.ethereum.org/EIPS/eip-1013
- https://github.com/goerli/testnet
- wss://back.01space.com.cn:8083/evadeKill/medal
- https://developer.apple.com/library/safari/documentation/AppleApplications/Reference/SafariHTMLRef/Articles/MetaTags.html--
- https://github.com/ethereum/ropsten
- https://kovan-testnet.github.io/website/
- https://eips.ethereum.org/EIPS/eip-608
- https://eips.ethereum.org/EIPS/eip-3198
- http://api.yunchengjihua.com/uploads/20240425/eedd39dd771b50f2a8962561d710d312.jpg
- https://eips.ethereum.org/EIPS/eip-1679
- https://cdn.dcloud.net.cn/img/shadow-grey.png
- https://01space.com.cn:8083/api/
- http://api.yunchengjihua.com
- https://links.ethers.org/v5-errors-
- https://eips.ethereum.org/EIPS/eip-1559
- https://eips.ethereum.org/EIPS/eip-2315
- wss://back.01space.com.cn:8083/eludeKill/gem
- https://intl.cloud.tencent.com/document/product/266/33942
- https://eips.ethereum.org/EIPS/eip-2929
- http://api.yunchengjihua.com:8089/api/
- https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf
- https://intl.cloud.tencent.com/document/product/266/33977
- wss://gema.chaowan.ink/evadeKill/minerals
- http://admin888.yunchengjihua.com/uploads/20240415/0904004691fc08477420ed0[illegible]c163db4d.png
- https://eips.ethereum.org/EIPS/eip-2537
- https://www.rinkeby.io
- http://www.html5rocks.com/en/mobile/mobifying/--
- https://gema.chaowan.ink/api/
- https://bsc-testnet.publicnode.com
- https://eips.ethereum.org/EIPS/eip-3541
- https://t.me/
- https://eips.ethereum.org/EIPS/eip-2565
- https://eips.ethereum.org/EIPS/eip-3675
- https://eips.ethereum.org/EIPS/eip-2070
- wss://gema.chaowan.ink/evadeKill/stoneNum
- https://github.com/crypto-browserify/crypto-brow[illegible]erify
- https://assets.salesmartly.com/js/project_32278_33600_1701143931.js
- http://api.yunchengjihua.com/uploads/20240414/1a4390b248ed91d0f239[illegible]dad3ebd2422.gif
- https://www.yimenapp.com/doc/echo2.cshtml?callback=?
- http://ycjh.yunchengjihua.com/
- https://github.com/videojs/video.js/issues/7617
- https://www.yimenapp.com/doc/demo_net.cshtml
- https://github.com/ethereum/pm/issues/361
- http://api.yunchengjihua.com/uploads/20240425/22b39b447ec91f8287b1f0608eb3947.png
- https://eips.ethereum.org/EIPS/eip-2930
- https://imgcache.qq.com/open_proj/proj_qcloud_v2/mc_2014/video/console/v2/css/img/vod/default-cover.png
- https://www.yimenapp.com/doc/echo.cshtml
- http://fontello.com
- wss://gema.chaowan.ink/evadeKill/medal
- https://cloud.tencent.com/document/product/266/34071
- http://api.yunchengjihua.com/uploads/20240425/f0aae3ed3f5e9e9b588f515355d95714.jpg
- https://github.com/ethereum/pm/issues/356
- https://eips.ethereum.org/EIPS/eip-3529
- https://eips.ethereum.org/EIPS/eip-1716
- https://eips.ethereum.org/EIPS/eip-606
- https://gema.chaowan.ink/
- wss://back.01space.com.cn:8083/eludeKill/medal
- http://admin.gailou1.22ceshi.com/uploads/20240314/1530ea0d5f39e17764f2a3df40346d96.png
- https://ethstats.net/
- https://xcity.cc
- https://twitter.com/LIBRA
- https://gate.myapp.ltd/cdn/jsbridge-mini.js

自研引擎-A

• http://admin888.yunchengjihua.com/uploads/20240416/b2f13c2e08838abeea7f7d41a753170f.png • https://datacenter.live.qcloud.com • https://drm.vod2.myqcloud.com/getlicense/v1 • https://eips.ethereum.org/EIPS/eip-2384 • http://admin888.yunchengjihua.com/uploads/20240416/3045d9b456b3fccbff883ab77087c7ad.png • https://eips.ethereum.org/EIPS/eip-2718 • https://vjs.zencdn.net/vttjs/0.12.4/vtt.min.js	
• 2.5.29.15	g/l/a/k.java
• https://www.baidu.com/favicon.ico?	com/lt/app/views/l0.java
• 8.8.8.8 • https://1.12.12.12/dns-query • 223.5.5.5 • 223.6.6.6 • https://dns.alidns.com/dns-query • 119.29.29.29	com/lt/plugin/l0.java
• 114.114.114.114	com/lt/plugin/a2/e.java
• javascript:window.webviewjavascriptbridgeinterface.onresultforscript	g/j/a/m.java
• 8.8.8.8 • https://1.12.12.12/dns-query • 223.5.5.5 • 223.6.6.6 • 114.114.114.114 • https://dns.alidns.com/dns-query • 2.5.29.15 • 119.29.29.29 • javascript:window.webviewjavascriptbridgeinterface.onresultforscript • https://www.baidu.com/favicon.ico?	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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
"http_auth_p" : "Password"
6148523063484D364C793965E4C6E6C706257567563325676 4C6D4E754C773D3D

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。