南明离火
移动应用检测平台

ANDROID 静态分析报告

安全生产 • v2.0.24030101

本报告由南明离火移动安全分析平台生成

分析日期: 2024-03-05 15:34:15

应用概览

文件名称:	Safe_24030101.apk
文件大小:	24.59MB
应用名称:	安全生产
软件包名:	com.westcn.www
主活动:	com.activity.base.WelcomeActivity
版本号:	2.0.24030101
最小SDK:	26
目标SDK:	34
加固信息:	360加固 加固
应用程序安全分数:	53/100 (中风险)
杀软检测:	AI评估：可能有安全隐患
MD5:	831513faae9a801caebd61a28eb2e60f
SHA1:	7aa78fcbe123eb6411b6d8ee5b49b4dba[illegible]b41276
SHA256:	1e3b2e34dcaef3a6219bf42c006e[illegible]2605424554b761768e76ee[illegible]e696b60b394

分析结果严重性分布

高危	中危	信息	安全	关注
1	4	0	1	0

四大组件导出状态统计

Activity组件：35个，其中export的有：0个
Service组件：1个，其中export的有：0个
Receiver组件：1个，其中export的有：1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: False
v2 签名: True
v3 签名: False

v4 签名: False
主题: C=86, ST=lanzhou, L=lanzhou, O=FEITIAN, OU=Lanzhou Feitian Wangjing Information Industry Co.Ltd, CN=www.westcn.com
签名算法: rsassa_pkcs1v15
有效期自: 2022-11-04 03:48:29+00:00
有效期至: 2047-10-29 03:48:29+00:00
发行人: C=86, ST=lanzhou, L=lanzhou, O=FEITIAN, OU=Lanzhou Feitian Wangjing Information Industry Co.Ltd, CN=www.westcn.com
序列号: 0x183f5c2d
哈希算法: sha256
证书MD5: 3934f90ea381ceaa8ef5cb4b8e6ad144
证书SHA1: 700453961739bc0900aca64d1f29b6fcc84b02c5
证书SHA256: d86894c2baf08b3d9bf933b510281b8a06e952142523946907e3977aaa3d92f2
证书SHA512:
37e98935a366ac89f31768a6c83e290acd559b930f8ebdd836684714d6a648bf829ef3446d42de81774d0b03111c286659da2e966ab1768a2[illegible]706bccd7515262

公钥算法: rsa
密钥长度: 2048
指纹: 4cfcd90acc089fc1b7f4eba7ea5e43270d4d0cda4ec0fc6e274c5cddcb209ac0
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.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.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_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.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.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_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.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.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.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.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_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.REORDER_TASKS	危险	对正在运行的应用程序重新排序	允许应用程序将任务移至前端和后台。恶意应用程序可借此强行进入前端，而不受您的控制。
com.westcn.www.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。

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: **0** | 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: **4** | 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存在漏洞的 Android 版本上 Android 8.0, minSdk=26]	警告	该应用程序可以安装在具有多个漏洞的旧版本 Android 上。支持 Android 版本 => 10、API 29 以接收处理的安全更新。
2	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
3	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。
4	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
5	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

代码安全漏洞检测

序号	问题	等级	参考标准	文件位置

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	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/libAMapSDK_MAP_v6_8_0.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/libmsec.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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	6/30	android.permission.CAMERA android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.VIBRATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.READ_PHONE_STATE
其它常用权限	8/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.READ_MEDIA_IMAGES android.permission.ACCESS_NETWORK_STATE android.permission.REORDER_TASKS android.permission.FLASHLIGHT

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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
upx.sf.net	安全	否	**IP地址:** 172.64.153.102 **国家:** United States of America **地区:** Texas **城市:** Dallas **纬度:** 32.783058 **经度:** -96.806671 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• http://upx.sf.net	lib/arm64-v8a/libAMapSDK_MAP_v6_8_0.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
360 加固	360	360 加固保是基于 360 核心加密技术，给安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包，内存抓取等威胁。

邮箱地址敏感信息提取

EMAIL	源码文件
framework@boot.oat framework@boot.art	lib/arm64-v8a/libmsec.so

免责声明及风险提示: