南明离火
移动应用检测平台

ANDROID 静态分析报告

Satoshi • v5.0.8

分析日期: 2024-05-18 21:28:39

应用概览

文件名称:	Satoshi-5080-GLO.apk
文件大小:	48.06MB
应用名称:	Satoshi
软件包名:	com.sat21.global.pro
主活动:	com.btcs.MainActivity
版本号:	5.0.8
最小SDK:	21
目标SDK:	33
加固信息:	Flutter/Dart 加固
应用程序安全分数:	46/100 (中风险)
跟踪器检测:	1/432
杀软检测:	经检测，该文件安全
MD5:	13ab9ccf7be6cd9cd9254f88e869bdeb
SHA1:	76b877ce4b0f63455894e4a1d[illegible]c8e1921c65
SHA256:	4224887b2f16fd0fa07672b1804e2391887a834963[illegible]2c42abd53997e2bf9854c

分析结果严重性分布

高危	中危	信息	安全	关注
1	2	1	0	1

四大组件导出状态统计

Activity组件：6个，其中export的有：1个
Service组件：1个，其中export的有：0个
Receiver组件：1个，其中export的有：0个
Provider组件：1个，其中export的有：1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
v4 签名: False
主题: C=cn, ST=zj, L=hz, O=hij, OU=def, CN=abc
签名算法: rsassa_pkcs1v15
有效期自: 2021-07-04 05:33:56+00:00
有效期至: 2121-06-10 05:33:56+00:00
发行人: C=cn, ST=zj, L=hz, O=hij, OU=def, CN=abc
序列号: 0xc8301a1
哈希算法: sha256
证书MD5: f1f4196cc4e3566e5e085420a0c65921
证书SHA1: 630798061571b17ab24a7a38182733a071aff910
证书SHA256: 088c78a3334a7f148c7f999bc975eb87e1d60968f04417cb4910a68b17edd83b
证书SHA512:
4354f622a89dc8a24b91e6b0fe15921246bb4d6d546c6738b9dcaf2255c7980ee91a3ad5ffb6b6bda4a8c0cdb4bdd1b6e703a7a82a4fca6af3b79bf91f96242d

公钥算法: rsa
密钥长度: 2048
指纹: 37418b4e3146a96a860694431ffc8918cb926ffec308f7be1937b30f2047d765
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.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.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.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.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.hardware.camera.autofocus	未知	未知权限	来自 android 引用的未知权限。
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.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.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.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.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。

网络通信安全风险分析

高危: **0** | 警告: **0** | 信息: **0** | 安全: **0**

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: **5** | 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 5.0-5.0.2, [minSdk=21]	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	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，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	Activity (com.baidu.liantian.LiantianActivity) 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。
6	Content Provider (com.baidu.liantian.LiantianProvider) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
7	高优先级的 Intent (2147483647) [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。

代码安全漏洞检测

高危: **1** | 警告: **5** | 信息: **1** | 安全: **0** | 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	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
4	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
5	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
6	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
7	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

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/libapp.so	False high 二进制文件没有设置NX位。NX位可以通过将内存页标记为不可执行来防止内存损坏漏洞被利用。使用选项-noexecstack或-znoexecstack来将栈标记为不可执行		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	Not Applicable info RELRO 检查不适用于 Flutter/Dart 二进制文件	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 info 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/libbd_unifylicense.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/libliantian.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: ['__sprintf_chk', '__snprintf_chk']	False warning 符号可用

4	arm64-v8a/libpaddle_light_api_shared.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	Partial RELRO warning 此共享对象启用了部分 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在部分 RELRO 中，GOT 部分的非 PLT 部分是只读的，但 .got.plt 仍然是可写的。使用选项 -z,relro,-z,now 启用完整的 RELRO。	/opt/android-ndk-r17c/toolchains/llvm/prebuilt/linux-x86_64/lib64/clang/6.0.2/lib/linux/aarch64 high 二进制文件设置了RPATH。在某些情况下，攻击者可以利用这个特性来运行任意的库，实现代码执行和提权。库应该设置RPATH的唯一情况是当它链接到同一个包中的私有库时。删除编译器选项-rpath来移除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	5/30	android.permission.CAMERA android.permission.READ_PHONE_STATE android.permission.WAKE_LOCK android.permission.WRITE_SETTINGS android.permission.ACCESS_FINE_LOCATION
其它常用权限	6/46	android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE 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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
bugs.llvm.org	安全	否	**IP地址:** 54.67.122.174 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 圣何塞 **纬度:** 37.339390 **经度:** -121.894958 **查看:** Google 地图

aip.baidubce.com	安全	是	**IP地址:** 180.97.107.95 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
openmp.llvm.org	安全	否	**IP地址:** 54.67.122.174 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 圣何塞 **纬度:** 37.339390 **经度:** -121.894958 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://ai.baidu.com/activation/key/activate	com/baidu/vis/unified/license/BDLicenseActivator.java
• 3.0.9.1	f/a/b/a/a/f.java
• 10.0.0.172 • 4.0.3.5 • https://dxp.baidu.com/upgrade • file:null • https://hmma.baidu.com/auto.gif • 3.0.9.1 • https://hmma.baidu.com/app.gif • http://datax.baidu.com/xs.gif • http://hmma.baidu.com/app.gif • https://datax.baidu.com/xs.gif • 10.0.0.200 • https://ai.baidu.com/activation/key/activate • http://dxp.baidu.com/upgrade • 3.5.7.5 • http://openrcv.baidu.com/1010/bplus.gif • https://openrcv.baidu.com/1010/bplus.gif	自研引擎-S
• https://aip.baidubce.com/public/2.0/license/face/app/querydevicelicense	lib/arm64-v8a/libbd_unifylicense.so
• http://openmp.llvm.org/ • https://bugs.llvm.org/	lib/arm64-v8a/libpaddle_light_api_shared.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
百度人脸识别	Baidu	人脸离线识别 SDK，包含人脸采集、活体检测、人脸对比/识别、人脸库管理等能力，并全部离线化、本地化。
Flutter	Google	Flutter 是谷歌的移动 UI 框架，可以快速在 iOS 和 Android 上构建高质量的原生用户界面。
C++ 共享库	Android	在 Android 应用中运行原生代码。

本报告由南明离火移动安全分析平台生成

Paddle Lite	Baidu	Paddle Lite 是一个高性能、轻量级、灵活性强且易于扩展的深度学习推理框架，定位于支持包括移动端、嵌入式以及边缘端在内的多种硬件平台。当前 Paddle Lite 不仅在百度内部业务中得到全面应用，也成功支持了众多外部用户和企业的生产任务。

第三方追踪器检测

名称	类别	网址
Baidu Mobile Stat	Analytics	https://reports.exodus-privacy.eu.org/trackers/101

敏感凭证泄露检测

可能的密钥
百度统计的=> "BaiduMobAd_CHANNEL" : "btc2100"
百度统计的=> "BaiduMobAd_STAT_ID" : "26291de706"
凭证信息=> "seckey_avscan" : "660346260f8a841a04ec2a56815b421b"
凭证信息=> "appkey_avscan" : "100034"

Google Play 应用市场信息

标题: Satoshi

评分: 4.309976 **安装:** 5,000,000+ **价格:** 0 **Android版本支持:** **分类:** 工具 **Play Store URL:** com.sat21.global.pro

开发者信息: Aimee Han, Aimee+Han, None, https://www.btcc.global, aimeemand666@gmail.com,

发布日期: None **隐私政策:** Privacy link

关于此应用:

中本聪致力于提供最专业、最准确、最快捷的报价和数据分析服务。借助全球分布的市场数据服务器，价格更新速度高达每秒十次，让我们的用户可以同时查看海量的全球信息。中本聪提供多维度分析，支持价格趋势分析，包括烛台图、HLC图、折线图，以及MACD/KDJ/RSI/BOLL/WR等专业分析指标。此外，市场资金流向监控允许用户查看每个时间段的资金流入和流出。

免责声明及风险提示：