南明离火
移动应用检测平台

ANDROID 静态分析报告

啊哈加速器 • v3.4.0

分析日期: 2024-05-13 14:29:51

应用概览

文件名称:	ahaspeed_android.apk
文件大小:	48.79MB
应用名称:	啊哈加速器
软件包名:	com.ahaspeed.app
主活动:	com.ahaspeed.app.MainActivity
版本号:	3.4.0
最小SDK:	21
目标SDK:	33
加固信息:	Flutter/Dart 加固
应用程序安全分数:	53/100 (中风险)
跟踪器检测:	1/432
杀软检测:	AI评估：安全
MD5:	4cc40a721166f63a510ca5045f68f9cb
SHA1:	17fb56d793b922f0c66142c79[illegible]18b3ba86
SHA256:	4620abb82c21162027f0c[illegible]4fa141b2d927b34b017331eb3857e13ac5cf91e7

分析结果严重性分布

高危	中危	信息	安全	关注
2	9	1	2	2

四大组件导出状态统计

Activity组件：3个，其中export的有：0个
Service组件：6个，其中export的有：0个
Receiver组件：2个，其中export的有：0个
Provider组件：1个，其中export的有：0个

应用签名证书信息

二进制文件已签名

本报告由南明离火移动安全分析平台生成

v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=CA, ST=ON, L=Markham, O=Web Industrial Solutions Inc., OU=IT, CN=KhimSing Lai
签名算法: rsassa_pkcs1v15
有效期自: 2021-10-22 22:28:24+00:00
有效期至: 2049-03-09 22:28:24+00:00
发行人: C=CA, ST=ON, L=Markham, O=Web Industrial Solutions Inc., OU=IT, CN=KhimSing Lai
序列号: 0x3a15378f
哈希算法: sha256
证书MD5: f650478e829302765723c3f6c2609910
证书SHA1: cf5c5310b741bd6f85aea1e34d5e13ef906310ba
证书SHA256: a818c8cedd3f20d71edc8c6148279123665fce81947bee2520152232a2529521
证书SHA512:
b9f561abb4e4455957c19477443b1ea7e14917819a14430f4fa018d053267824ddbf5e5070ae66c401bd1677693c5e444a23192f3a869412b1bb2f28ff2f57e

公钥算法: rsa
密钥长度: 2048
指纹: b295b46be795710a5342375bb036c8852cf45db9e4228f4152a3a6fec96783ba
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.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.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.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.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_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_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以衡量广告活动的有效性。
android.permission.ACCESS_ADSERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
com.ahasoftec.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.android.vending.BILLING	普通	应用程序具有应用内购买	允许应用程序从 Google Play 进行应用内购买。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.ahaspeed.app.MainActivity	Schemes: http://, https://, Hosts: ahaspeed.com,

网络通信安全风险分析

高危: **0** | 警告: **1** | 信息: **0** | 安全: **1**

序号	范围	严重级别	描述
1	*	安全	基本配置配置为禁止到所有域的明文流量。
2	*	警告	基本配置配置为信任系统证书。

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: **1** | 警告: **0** | 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	App Link assetlinks.json 文件未找到 [android:name=com.ahaspeed.app.MainActivity] [android:host=http://ahaspeed.com]	高危	App Link 资产验证 URL （http://ahaspeed.com/.well-known/assetlinks.json ） 未找到或配置不正确。（状态代码：301）。应用程序链接允许用户从 Web URL/电子邮件重定向到移动应用程序。如果此文件丢失或为 App Link 主机/域配置不正确，则恶意应用程序可以劫持此类 URL。这可能会导致网络钓鱼攻击，泄露 URI 中的敏感数据，例如 PII、OAuth 令牌、魔术链接/密码重置令牌等。您必须通过托管 assetlinks.json 文件并通过 Activity intent-filter 中的 [android：autoVerify="true"] 启用验证来验证 App Link 网域。

代码安全漏洞检测

高危: **1** | 警告: **0** | 信息: **1** | 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	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	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
5	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
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	升级会员：解锁高级权限
8	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
9	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

本报告由南明离火移动安全分析平台生成

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	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	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/libnetapi.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: ['__vsnprintf_chk', '__strlen_chk', '__strncat_chk', '__read_chk', '__memmove_chk']	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	3/30	android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	7/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.READ_EXTERNAL_STORAGE com.google.android.gms.permission.AD_ID com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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
google.com	安全	否	**IP地址:** 142.250.76.142 **国家:** 日本 **地区:** 东京 **城市:** 东京 **纬度:** 35.689499 **经度:** 139.692322 **查看:** Google 地图

app-measurement.com	安全	是	**IP地址:** 180.163.150.161 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
goo.gl	安全	否	**IP地址:** 142.250.76.142 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
api.flutter.dev	安全	否	**IP地址:** 180.163.150.161 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
pagead2.googlesyndication.com	安全	是	**IP地址:** 180.163.150.161 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• 223.5.5.5 • 10.10.10.6	com/ahaspeed/app/VPNetwork.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	k0/b.java
• https://%s/%s/%s	l2/c.java
• 10.10.10.6	r/b.java
• https://github.com/flutter/packages/blob/main/packages/in_app_purchase/in_app_purchase/README.md#loading-products-for-sale	v3/i.java

• https://goo.gl/naoooi • https://app-measurement.com/a • https://github.com/flutter/packages/blob/main/packages/in_app_purchase/in_app_purchase/readme.md#loading-products-for-sale • https://firebase.google.com/docs/analytics • https://www.google.com • https://firebase.google.com/support/privacy/init-options • https://firebase.google.com/support/guides/disable-analytics • 10.10.10.6 • 223.5.5.5 • https://google.com/search? • https://%s/%s/%s • https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps • www.google.com	自研引擎-S
• https://api.flutter.dev/flutter/material/scaffold/of.html	lib/arm64-v8a/libapp.so
• 127.0.0.1 • 127.255.255.255 • 10.255.255.255 • 192.168.255.255	lib/arm64-v8a/libnetapi.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。
Google Play Billing	Google	Google Play 结算服务可让您在 Android 上销售数字内容。本文档介绍了 Google Play 结算服务解决方案的基本构建基块。要决定如何实现特定的 Google Play 结算服务解决方案，您必须了解这些构建基块。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。

第三方追踪器检测

名称	类别	网址
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

敏感凭证泄露检测

可能的密钥
"google_api_key" : "AIzaSyDw189d24XWCLsY8o8n53RmG0l2C-UFPlo"
"google_crash_reporting_api_key" : "AIzaSyDw189d24XWCLsY8o8n53RmG0l2C-UFPlo"
VGhpcyBpcyB0aGUga2V5IGZvcihBIHNlY3XyZZBzdG9yYWdlIEFFUyBLZXkK
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
VGhpcyBpcyB0aGUga2V5IGZvciBhIHNlY3VyZSBzdG9yYWdlIEFFUyBLZXkK
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBhIHNlY3VyZSBzdG9yYWdlCg

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。