南明离火
移动应用检测平台

ANDROID 静态分析报告

GENIEX Service • v2.2.062

分析日期: 2024-09-28 13:53:15

应用概览

文件名称:	com.geniex.vsimhelper v2.2.062.apk
文件大小:	3.02MB
应用名称:	GENIEX Service
软件包名:	com.geniex.vsimhelper
主活动:	com.skyroam.silverhelper.MainActivity
版本号:	2.2.062
最小SDK:	29
目标SDK:	33
加固信息:	未加壳
应用程序安全分数:	48/100 (中风险)
跟踪器检测:	1/432
杀软检测:	经检测，该文件安全
MD5:	13dc6b335e0f136597784161f314cd8e
SHA1:	605af51fcf57736a4647efb19[illegible]7699039300f4
SHA256:	f8cecf86a1a70f7d1195e0f08319c62a6732e14192e9131912df764e9f8304c5

分析结果严重性分布

高危	中危	信息	安全	关注
2	2	1	1	2

四大组件导出状态统计

Activity组件：1个，其中export的有： 0个
Service组件：2个，其中export的有： 2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

v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=CN, ST=Shanghai, L=Shanghai, O=TecnoMobile, OU=HiOS, CN=HiOS, E=hios@tecno-mobile.com
签名算法: rsassa_pkcs1v15
有效期自: 2019-04-16 07:56:33+00:00
有效期至: 2046-09-01 07:56:33+00:00
发行人: C=CN, ST=Shanghai, L=Shanghai, O=TecnoMobile, OU=HiOS, CN=HiOS, E=hios@tecno-mobile.com
序列号: 0xf77a779d3b53f452
哈希算法: sha256
证书MD5: 4e0244ab4cf7f14ee58378e017e903ed
证书SHA1: aec83f63bfa3a6ad9422086688639fea7684ef00
证书SHA256: 40e4400c5c90f79d8f390584eebad893ac9bdba0ff1507b126d4c9db547929da
证书SHA512:
77fd51980f1e14166f4a50953b7c7eba1f144e9c6bf6476eb03c28852d2e341f1e1efc989c078348b4a6aa93c43d07e59b83614503947386758051c5960948c

公钥算法: rsa
密钥长度: 2048
指纹: 84d7ca7eca4fdf87cf3ac1728ffdf3e50f40483525cff5e51b24846c2648a7f7
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.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.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.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
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.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.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_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.READ_PRECISE_PHONE_STATE	危险	允许以只读方式访问精确的电话状态	允许只读访问精确的电话状态。允许读取特殊用途应用程序（如拨号器、运营商应用程序或ims应用程序）的电话状态详细信息。
android.permission.MODIFY_PHONE_STATE	签名(系统)	修改手机状态	允许应用程序控制设备的电话功能。拥有此权限的应用程序可自行切换网络、打开和关闭无线通信等，而不会通知您。
android.permission.WRITE_APN_SETTINGS	危险	写入访问点名称设置	允许应用程序写入访问点名称设置。
android.permission.CONNECTIVITY_INTERNAL	未知	未知权限	来自 android 引用的未知权限。
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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
com.transsion.dataservice.permission.READ	未知	未知权限	来自 android 引用的未知权限。
com.transsion.dataservice.permission.WRITE	未知	未知权限	来自 android 引用的未知权限。
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。
com.google.android.providers.gsf.permission.READ_GSERVICES	未知	未知权限	来自 android 引用的未知权限。
com.geniex.vsimhelper.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全合规分析

高危: **1** | 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: **1** | 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。
2	应用程序处于测试模式 [android:testOnly=true]	高危	它可能会暴露自身之外的功能或数据，这会造成一个安全漏洞。
3	Service (com.skyroam.silverhelper.msp.SilverService) 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，因此可被设备上的任何其他应用程序访问。
4	Service (com.skyroam.silverhelper.msp.MainService) 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，因此可被设备上的任何其他应用程序访问。

5	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: **6** | 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
3	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
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	升级会员：解锁高级权限
5	MD5是已知存在哈希冲突的算法	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	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
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

8	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
9	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	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.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK android.permission.READ_PHONE_STATE android.permission.WRITE_SETTINGS
其它常用权限	7/46	android.permission.INTERNET android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS com.google.android.gms.permission.AD_ID

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
connectivitycheck.platform.hicloud.com	安全	是	**IP地址:** 23.59.157.13 **国家:** 中国 **地区:** 江苏 **城市:** 常州 **纬度:** 31.783331 **经度:** 119.966667 **查看:** 高德地图
gslb.shalltry.com	安全	否	**IP地址:** 23.59.157.13 **国家:** 爱尔兰 **地区:** 都柏林 **城市:** 都柏林 **纬度:** 53.344151 **经度:** -6.267249 **查看:** Google 地图

gx-api.geniex.com	安全	否	**IP地址:** 23.59.157.13 **国家:** 尼日利亚 **地区:** 拉各斯 **城市:** 拉各斯 **纬度:** 6.452972 **经度:** 3.395816 **查看:** Google 地图
ire-oneid.shalltry.com	安全	否	**IP地址:** 23.59.157.13 **国家:** 德国 **地区:** 黑森 **城市:** 美因河畔法兰克福 **纬度:** 50.110882 **经度:** 8.681996 **查看:** Google 地图
data-api.geniex.com	安全	否	**IP地址:** 23.59.157.13 **国家:** 尼日利亚 **地区:** d Islands [Malvinas]FM Micronesia (Federated States of)FO Faroe IslandsFRFranceGAGabonGB4United Kingdom **城市:** 拉各斯 **纬度:** 6.452972 **经度:** 3.395816 **查看:** Google 地图
osi-api.geniex.com	安全	否	**IP地址:** 152.32.143.31 **国家:** 尼日利亚 **地区:** 拉各斯 **城市:** 拉各斯 **纬度:** 6.452972 **经度:** 3.395816 **查看:** Google 地图
www.pool.ntp.org	安全	否	**IP地址:** 151.101.193.55 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
time.cloudflare.com	安全	否	**IP地址:** 151.101.193.55 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
manual.sensorsdata.cn	安全	是	**IP地址:** 180.97.251.233 **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

captive.apple.com	安全	否	**IP地址:** 23.59.157.13 **国家:** 加拿大 **地区:** 不列颠哥伦比亚省 **城市:** 温哥华 **纬度:** 49.240822 **经度:** -123.116714 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• 1.1.0.1 • 2.3.6.0	自研引擎-M
• http://osi-api.geniex.com/simo/user/public/getauthcode • https://data-api.geniex.com/sa?project=production • https://data-api.geniex.com/sa?project=default • https://gx-api.geniex.com	com/skyroam/silverhelper/MyApplication.java
• 223.5.5.5	b2/g.java
• https://ire-oneid.shalltry.com	l2/e.java
• 1.1.0.1 • https://gslb.shalltry.com/gslb/domain/convert	m2/g.java
• 223.5.5.5	o1/d.java
• 223.5.5.5	b2/b.java
• http://captive.apple.com/hotspot-detect.html • http://connectivitycheck.platform.hicloud.com/generate_204	d2/j.java
• https://ire-oneid.shalltry.com	v2/g.java
• https://time1.google.com • https://time.cloudflare.com • https://www.pool.ntp.org	t0/c.java
• http://captive.apple.com/hotspot-detect.html • http://connectivitycheck.platform.hicloud.com/generate_204	d2/h.java
• 2.5.29.15	z0/e.java

• https://data-api.geniex.com/sa?project=production • https://gslb.shalltry.com/gslb/domain/convert • 2.5.29.15 • https://ire-oneid.shalltry.com • http://osi-api.geniex.com/simo/user/public/getauthcode • javascript:window.sensorsdata_app_call_js • https://time.cloudflare.com • http://connectivitycheck.platform.hicloud.com/generate_204 • https://www.pool.ntp.org • https://gx-api.geniex.com • https://manual.sensorsdata.cn/sa/latest/tech_sdk_client_web_use-7545346.html • 223.5.5.5 • http://captive.apple.com/hotspot-detect.html • https://time1.google.com • https://data-api.geniex.com/sa?project=default • 1.0.2.1 • 1.1.0.1	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
神策分析 SDK	神策	神策分析，是针对企业级客户推出的深度用户行为分析产品，支持私有化部署，客户端、服务器、业务数据、第三方数据的全端采集和建模，驱动营销渠道效果优化、用户精细化运营改进、产品功能及用户体验优化、老板看板辅助管理决策、产品个性化推荐改造、用户标签体系构建等应用场景。作为 PaaS 平台支持二次开发，可通过 BI、大数据平台、CRM、ERP 等内部 IT 系统，构建用户数据体系，让用户行为数据发挥保值的价值。
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 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。

第三方追踪器检测

名称	类别	网址
Sensors Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/248

敏感凭证泄露检测

可能的密钥
nCGSS6NKf4glPrFbTM97xE9ZKGUiMALIV8W7FClAgLZdtTZkL5XEQdbX4RB/C6edc
nzFx18H12iZ9gGVzMbHetvImBoXeCOwjTc5RnGIz+Hya96pxJLK2DcSlAaHEs1H
3b0b10346b28d9d6ce83c6265bcb5bb
861b5972a3555dbda8b8d9dbc6115a64

76iRl07s0xSN9jqmEWAt79EBJZuIIQIsV64FZr2O
nnN2ifla6sVu23y78FMiL6smp9ayE7Y3gSEfB3md4nvEUpyRUu4wYLIf9nVR36okK
nGCerxYdLtDbJ69Rux4lgE5C9a6qLfV6BzjJYONk/vQhGQYT6qes+TFtXV0hvF8UM
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArNrm4jErOdstd1P5L1X/
63D4BEBEBC7ABCA4BC6A796B6AB06B766A6C7D706B6B756F70B07B6F71A4A5AEBCB2D4BEBEBC6A69BCA4BC7A6B69B16A796B6AB06B767D72726A6C65B07B6F71BCB2D4BEBEBC6A7BBCA4BC7A6B7BB16A796B6AB06B767D72726A6C65B07B6F71BCB2D4BEBEBC6F69BCA4BC7A6B69B06B767D72726A6C65B07B6F71BCB2D4BEBEBC6F7BBCA4BC7A6B7BB06B767D72726A6C65B07B6F71BCB2D4BEBEBC7BBCA4BCAF726F777B6F7078AF68A8AF696E726F7D7A7B6F7078BCB2D4BEBEBC77BCA4BCAF726F777B6F7078AF68ADAF6B797B6C796ABCB2D4BEBEBC69BCA4BCAF7D6A7679707DAF7B76797B736E6F75706AAF68ACAF696E726F7D7ABCB2D4BEBEBC787BBCA4BC68AEAC7BBCB2D4BEBEBC787ABCA4BC68AEAC7ABCB2D4BEBEBC7879BCA4BC68AEAC79BCB2D4BEBEBC7568BCA4BC7D7C7B7A79787776757473AD71706F6EBCB2D4BEBEBC67BCA4BCABA7ADA899A9CB9CAD9CA5A6AC9BAEABA9AEADAB99A9ACADA8A79D9D98A9AA9DBCD461D4D4

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，深入扫描软件中潜在的漏洞和安全隐隐患。