南明离火
移动应用检测平台

ANDROID 静态分析报告

Mew • v1.1.3

分析日期: 2024-05-03 06:44:30

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

应用概览

文件名称:	Mewv1.1.3.apk
文件大小:	8.36MB
应用名称:	Mew
软件包名:	cl.datacomputer.alejandrob.newgpsjoysticl
主活动:	cl.datacomputer.alejandrob.newgpsjoysticl.SplashScreenActivity
版本号:	1.1.3
最小SDK:	18
目标SDK:	23
加固信息:	未加壳
应用程序安全分数:	41/100 (中风险)
跟踪器检测:	5/432
杀软检测:	3 个杀毒软件报毒
MD5:	2c97fc89b634adccdf2e096067417e16
SHA1:	38ac266cc0127cc00c1c1272a30a5dd0b0131d4e3
SHA256:	3ef88cf8ef5f7ba73fa449418abb8801d58feafc2b5128944297374b35c2cbd

分析结果严重性分布

高危	中危	信息	安全	关注
5	3	3	0	5

四大组件导出状态统计

Activity组件：13个，其中export的有：1个
Service组件：7个，其中export的有：5个
Receiver组件：4个，其中export的有：3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

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: False
v3 签名: False
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea3039772720179587d04d89b7711292a4569

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.ACCESS_MOCK_LOCATION	危险	获取模拟定位信息	获取模拟定位信息，一般用于帮助开发者调试应用。恶意程序可以用它来覆盖真实位置信息源。
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.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_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.WRITE_SECURE_SETTINGS	签名(系统)	修改安全系统设置	允许应用程序修改系统的安全设置数据。普通应用程序不能使用此权限。
android.permission.CHANGE_COMPONENT_ENABLED_STATE	签名(系统)	启用或禁用应用程序组件	允许应用程序更改是否启用其他应用程序的组件。恶意应用程序可借此停用重要的手机功能。使用此权限时务必谨慎，因为这可能导致应用程序组件进入不可用、不一致或不稳定的状态。
android.permission.INSTALL_LOCATION_PROVIDER	签名(系统)	安装位置提供商	创建用于测试的模拟位置信息源。恶意程序可以用它来覆盖由真实位置信息源，如GPS或网络提供商返回的位置或状态，或者监视和报告您的位置到外部源
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.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令，恶意应用程序可能会使用它来干扰GPS或其他位置源的操作。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

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。
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.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。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
cl.datacomputer.alejandrob.newgpsjoysticl.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
cl.datacomputer.alejandrob.newgpsjoysticl.SplashScreenActivity	Schemes: http://, https://, Hosts: www.google.com, Mime Types: text/plain, Path Prefixes: /main,

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
应用程序存在Janus漏洞	高危	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

Manifest 配置安全分析

高危: **1** | 警告: **12** | 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 4.3-4.3.1, [minSdk=18]	警告	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。

本报告由南明离火移动安全分析平台生成

3	Service (cl.datacomputer.alejandrob.newgpsjoysticl.NewGpsFirebaseMessagingService) 未被保护。 存在一个intent-filter。	警告	发现 Service与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Service是显式导出的。
4	Service (cl.datacomputer.alejandrob.newgpsjoysticl.NewGpsFirebaseInstanceIDService) 未被保护。 存在一个intent-filter。	警告	发现 Service与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Service是显式导出的。
5	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
6	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	警告	发现一个 Service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。
7	Service (com.google.firebase.messaging.FirebaseMessagingService) 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，因此使其对设备上的任何其他应用程序都可访问。
8	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。
9	Service (com.google.firebase.iid.FirebaseInstanceIdService) 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，因此使其对设备上的任何其他应用程序都可访问。
10	Content Provider (com.applisto.appcloner.classes.DefaultProvider) 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，因此使其对设备上的任何其他应用程序都可访问。
11	Broadcast Receiver (com.applisto.appcloner.classes.DefaultProvider$DefaultReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

12	Activity (com.applisto.appcloner.classes.DefaultProvider$MyActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (23) 更新到 29 或更高版本以在平台级别修复此问题。
13	Activity (com.applisto.appcloner.classes.DefaultProvider$MyActivity) 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，因此使其对设备上的任何其他应用程序都可访问。

代码安全漏洞检测

高危: **2** | 警告: **10** | 信息: **3** | 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	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
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	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
5	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
6	不安全的WebView实现。可能存在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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

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	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
9	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
10	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
11	向Firebase上传数据	警告		升级会员：解锁高级权限
12	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
13	默认情况下，调用Cipher.getInstance("AES")将返回AES ECB模式，众所周知，ECB模式很弱，因为它导致相同明文块的密文相同	高危	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-2	升级会员：解锁高级权限
14	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
15	此应用侦听剪贴板更改。一些恶意软件也会监听剪贴板更改	信息	OWASP MASVS: MSTG-PLATFORM-4	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
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/libAndHook.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。		False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项-fstack-protector-all来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了Dart FFI	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	No 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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

2	arm64-v8a/libAndHookCompat.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。		False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项-fstack-protector-all来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了Dart FFI	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.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.WRITE_SETTINGS android.permission.VIBRATE android.permission.SYSTEM_ALERT_WINDOW android.permission.WAKE_LOCK
其它常用权限	7/46	android.permission.ACCESS_MOCK_LOCATION android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.ACCESS_NETWORK_STATE com.google.android.c2dm.permission.RECEIVE

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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

twitter.com	安全	否	**IP地址:** 104.244.42.193 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.773968 **经度:** -122.410446 **查看:** Google 地图
app-measurement.com	安全	是	**IP地址:** 180.163.150.166 **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
www.linkedin.com	安全	是	**IP地址:** 180.163.150.166 **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
example.com	安全	否	**IP地址:** 104.244.42.193 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
graph-video.s	安全	否	No Geolocation information available.
googleads.g.doubleclick.net	安全	是	**IP地址:** 180.163.150.166 **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:** 172.217.175.46 **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
www.paypal.com	安全	是	**IP地址:** 192.229.232.89 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.157692 **查看:** 高德地图

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

hellxenvenom.ddns.net	安全	否	**IP地址:** 104.244.42.193 **国家:** 智利 **地区:** 贝尔纳多·奥希金斯将军 **城市:** 兰卡瓜 **纬度:** -34.170830 **经度:** -70.744438 **查看:** Google 地图
pagead2.googlesyndication.com	安全	是	**IP地址:** 180.163.150.166 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.469433 **查看:** 高德地图
datacomputer.cl	安全	否	No Geolocation information available.
admob-app-id-2141153678.firebaseio.com	安全	否	**IP地址:** 35.190.39.113 **国家:** 美利坚合众国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
login.yahoo.com	安全	否	**IP地址:** 124.108.115.75 **国家:** 台湾省 **地区:** 台北 **城市:** 台北 **纬度:** 25.038172 **经度:** 121.563599 **查看:** Google 地图
www.firebase.com	安全	否	**IP地址:** 151.101.1.195 **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
www.datacomputer.cl	安全	否	No Geolocation information available.
graph.s	安全	否	No Geolocation information available.
www.twitter.com	安全	否	**IP地址:** 20.190.144.166 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.773968 **经度:** -122.410446 **查看:** Google 地图
facebook.com	安全	否	**IP地址:** 104.244.42.193 **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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

login.live.com	安全	否	**IP地址:** 20.190.144.166 **国家:** 大韩民国 **地区:** 首尔teukbyeolsi **城市:** 首尔 **纬度:** 37.566311 **经度:** 126.977203 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• www.google.com	自研引擎-M
• http://www.datacomputer.cl • www.datacomputer.cl	cl/datacomputer/alejandrob/newgpsjoysticl/AboutActivity.java
• http://datacomputer.cl/rest/sync/ver_solicitudesaddtojson.php • http://datacomputer.cl/rest/sync/ver_solicitudesadd.php	cl/datacomputer/alejandrob/newgpsjoysticl/AdministratorFragment.java
• https://m.facebook.com/gogpsapp/ • www.datacomputer.cl/privacy-policy.html • http://datacomputer.cl • http://datacomputer.cl/rest/sync/getdbrowcountdos.php • http://datacomputer.cl/rest/sync/solicitud.php • http://www.twitter.com/hell_envenom • https://play.google.com/store/apps/details?id=cl.datacomputer.alejandrob.newgpsjoysticl • http://datacomputer.cl/rest/pokeparadas.php • http://datacomputer.cl/rest/gimnasios.php • http://datacomputer.cl/rest/sync/obtener_pokestop_and_gyms_compressed.php • http://datacomputer.cl/rest/sync/lastupload.php • http://datacomputer.cl/rest/sync/newfile.json • http://datacomputer.cl/rest/sqlite/updatesyncsts.php • http://datacomputer.cl/rest/sync/obtener_pokestop.php • http://datacomputer.cl/rest/sync/addpokestoporgym.php	cl/datacomputer/alejandrob/newgpsjoysticl/MainActivity.java
• http://datacomputer.cl/rest/pokeparadas.php • http://datacomputer.cl/rest/gimnasios.php • http://datacomputer.cl/rest/token.php • file:///android_res/drawable/devgif.gif	cl/datacomputer/alejandrob/newgpsjoysticl/MapsIntineraryViewActivity.java
• http://datacomputer.cl/rest/sync/addpokestoporgym.php • http://datacomputer.cl	cl/datacomputer/alejandrob/newgpsjoysticl/VentanaFlotante.java
• http://datacomputer.cl/rest/sync/obtener_pokestop.php	cl/datacomputer/alejandrob/newgpsjoysticl/sqlite/BackgroundTask.java
• http://datacomputer.cl/rest/sync/obtener_gyms.php	cl/datacomputer/alejandrob/newgpsjoysticl/sqlite/BackgroundTaskGym.java
• http://datacomputer.cl/rest/sync/getdbrowcount.php	cl/datacomputer/alejandrob/newgpsjoysticl/sqlite/SampleBC.java
• 127.0.0.1	com/mongodb/ServerAddress.java
• 127.0.0.1	com/mongodb/gridfs/CLI.java

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

- http://datacomputer.cl/rest/gimnasios.php
- https://login.yahoo.com
- http://datacomputer.cl/rest/sync/addpokestoporgym_.php
- http://hellxenvenom.ddns.net:8080/rest-1.0/api/webservice/getrecords/
- http://play.google.com/store/apps/details?id=com.facebook.orca
- http://datacomputer.cl/rest/sync/obtener_gyms.php
- http://datacomputer.cl
- http://datacomputer.cl/rest/sync/getdbrowcountdos.php
- http://hellxenvenom.ddns.net:8080/rest-1.0/api/webservice/insertuser/
- https://www.firebase.com/docs/android/guide/offline-capabilities.html#section-handling-transactions-offline
- https://accounts.google.com
- https://graph.%s
- https://twitter.com
- https://www.paypal.com
- 8.8.4.4
- https://www.linkedin.com
- http://www.datacomputer.cl
- www.datacomputer.cl
- 8.8.8.8
- http://datacomputer.cl/rest/sqlite/updatesyncsts.php
- https://m.facebook.com/gogpsapp/
- 127.0.0.1
- www.datacomputer.cl/privacy-policy.html
- http://datacomputer.cl/rest/pokeparadas.php
- https://.facebook.com
- http://datacomputer.cl/rest/sync/addpokestoporgym.php
- https://facebook.com
- http://datacomputer.cl/rest/sync/solicitud.php
- http://www.twitter.com/hell_envenom
- http://datacomputer.cl/rest/sync/ver_solicitudesadd.php
- 127.0.0.255
- https://sb-ssl.google.com/safebrowsing/clientreport/malware
- www.google.com
- http://www.google.com
- https://pagead2.googlesyndication.com/pagead/gen_204
- http://datacomputer.cl/rest/sync/obtener_pokestop.php
- http://plus.google.com/
- https://www.facebook.com
- http://datacomputer.cl/rest/sync/ver_solicitudesaddtojson.php
- http://datacomputer.cl/rest/tokml.php
- https://goo.gl/fzriuv
- http://datacomputer.cl/rest/sync/getdbrowcount.php
- https://play.google.com/store/apps/details?id=cl.datacomputer.alejandrob.newgpsjoysticl
- http://datacomputer.cl/rest/sync/newfile.json
- https://login.live.com
- file:///android_res/drawable/devgif.gif
- https://admob-app-id-21411153678.firebaseio.com
- http://datacomputer.cl/rest/sync/editmylocations.php
- http://datacomputer.cl/rest/sync/lastupload.php
- https://app-measurement.com/a
- http://datacomputer.cl/rest/sync/obtener_pokestop_and_gyms_compressed.php
- https://graph-video.%s
- http://datacomputer.cl/rest/likeanddislike.php

自研引擎-S

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

Firebase 配置安全检测

标题	严重程度	描述信息

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Google Sign-In	Google	允许使用 Google 登录的 API。
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
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。
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。

邮箱地址敏感信息提取

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

EMAIL	源码文件
alejandro.burgos.c@gmail.com datacomputerapps@gmail.com ag2r.2x@gmail.com	cl/datacomputer/alejandrob/newgpsjoysticl/MainActivity.java
support@firebase.com alejandro.burgos.c@gmail.com ag2r.2x@gmail.com datacomputerapps@gmail.com	自研引擎-S

第三方追踪器检测

名称	类别	网址
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
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
凭证信息=> "com.google.android.geo.API_KEY" : "@string/google_maps_key"
"firebase_database_url" : "https://admob-app-id-21[illegible]53678.firebaseio.com"
"google_directions_key" : "AIzaSyAHBgcmgMApzU0TI55OIrQNISsU91GY6ZY"
"google_crash_reporting_api_key" : "AIzaSyB25ZrBw1ICyW74TCAyN6dNtaCYZ4chP8Q"
"google_api_key" : "AIzaSyB25ZrBw1ICyW74TCAyN6dNtaCYZ4chP8Q"
"google_maps_key" : "AIzaSyD5gGrXHtdW63hzLA_RSYv[illegible]d635x18UdzU"
n+AxcP7sT90e4w[illegible]lRLoVkh6KOeOs1Z8IekeSc[illegible]yWOWpL9T0tglaWGb+w/x8OmdyoJXQPCPkDTc
n78C8qo[illegible]wXwOcK9V1kHzIi2qlRGL[illegible]DSVx3KgP3rEWSlxHzAZt8OgljPjEvkcWGJmr4dyoA/A
noCasBeYxdhEKpQwBfJ50pb7y[illegible]2a[illegible]gN[illegible]ki7C4F0QoQ4DC2slIhFm4VchWLJb0nGeaa3F9QicidEUf
nzHYAd4WORoWsA241[illegible]kh[illegible]gw8j[illegible]6SHgPuC+lQifwMvAu8ZGavhnYmptVM+CLc4RUzgEm42eiehP2E
Y29tLmFwcGxpc3RvLmFwcGNsb25lci5jbGFzc2VzLnNlY29uZGFyeQ==
AIzaSyAHBgcmgMApzU0TI55OIrQNISsU91GY6ZY
nlwr5ETjez3RsKULS6ZJWAU8xvoIPcBxwGQRaC5I0iNvycX7oSARkPgQQQNKjwHJgQugIBGYiVLwY
n2olwU2SXZdN1AtzmEfwtI+49oSQRspqj1yT9EUqAMoahx3rYvpW8MLONwFzglxT7WyQ97eOMmX0M

本报告由南明离火移动安全分析平台生成

nJBUhcameExFCkEhow4NEJCIST32oW4TEg3ogbg+NkIAaSI1KFG2lNGIJimqU0/P3sGZ0nLNn9qx9
nxtAB6Dkkzc+55W9DaF97Fkkv5BBgPHxbUjgkvZgS+F2SbgztX10o9cGJpAXA1cB03BOr94DIZvZT
n+ZGkpzrId6ak3RlpLm1xz5kePn0QOrZ5A3H9GIMf80wHeZ+l7OZo6Qh7HwFWh45t3iCsKEiATkXo
nbz2PpFXK5obQPvYskh5WPqaG9rXnkDRR0q6cAjxZdP59oQNQA84ADshpO6vozBsB4DAP2/2KzrwR
n4EPbNtXMNgNzgO0pJjfLc54Q9QnnUoOaUIYAPh3VtjxGkQhzM+wXdSDCxzgR/iipbLkIXQNuy2sY
nd7qkHRn2vssMU5VdE3xYVka86jITBsDMNuBGM2mjDa9lhqhj7ifnqmsbvLfG5CH0PGDUkNXMvqV4
n6ILXhSq+P2Ae7qsIh4HV0REDDQ314F/QQmVQhaYmuwAAAABJRU5ErkJggg==
nAP7xsB0qOvNGAL+5kIrOvBGghKD60AgQmEYAONDD9oSiM98ndOlrwNdAPL4fjn7G/UKyedoX+C60
5e8f16062ea3cd2c4a0d547876baa6f38cabf625
nnEP6ewBXAAflTa7oYJUhwJEetmtGlXCvCL+m3LNYblk7NznmCXnpivcDfARoGWQz+wH3PlZaTRjs
nCXBIWXMAAC4jAAAuIwF4pT92AAAHk0lEQVR42u2dW6wdUxjHf98pirqURElc6tIihKZOL0rqLiEl
3i2ndDfv2rTHiSisAbouNdArYfORhtTPEefj3q2f
73966D8572D9D979B7187BCD62ECC4C7
n5cgy1k4ASf3A5cAFuJXKKaF9KpBPgDvM7KP4g1oIIGkCMADcBJwb2p8KOMvMPcUaCC3pALgfmBba
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
nZWtL6D4gxleEjTgRsiZreZ8nNC9qRwx6BC0WIWuyNpCzY/YJalfUgLFw4LPgFs0T+snumNuJ4BOL
nJ2k5MBi65DXhQ6iwE5b0BHBP6FLXhB3AUWa2u5ImSNKdNMFPcp2Z7YYKaoCkmcDa0CWuCYuBu8zs
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
njY7OJr0mLOpwiHpt4BgUi6Q3PCZi8h1SSjpR0vaM9LxEkHSMh69dMRHz7agGfUSlhqnzKG50dHiJ
nEWYD347Bz/VmtmYM96cSWoCWRCLMJvsE38naNXQ+k30gdExyJ+rV+3Z1fpu0Jssdnp1GWxEkHSTp
nYfAXeebVnyGCJC3JuHeGh1/vEx2hMjvh++m8iTvax9jMPgHOBv5OMXlE0tICyhR86SYXchted46h
nbmhoaGhoaMig8M5S0h7gENxxYMk8kg9v+nAPg34vs79CB6GnkDt8Q5KGon97Er8nPxu1LWU8UsbB
nsw0NDQ0NDQ0FUeshYpIOBE4BTsKt2ewLTEyYQCfK0MfeUYzYO8ROjmQsca3o2lrYFJm2AXuAL81s

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

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患。

© 2025 南明离火 - 移动安全分析平台自动生成