南明离火
移动应用检测平台

ANDROID 静态分析报告

GetWay • v1.1.26

分析日期: 2024-09-28 12:30:57

i应用概览

文件名称:	get.way.com v1.1.26.apk
文件大小:	8.96MB
应用名称:	GetWay
软件包名:	get.way.com
主活动:	get.way.com.MainActivity
版本号:	1.1.26
最小SDK:	21
目标SDK:	34
加固信息:	未加壳
应用程序安全分数:	50/100 (中风险)
跟踪器检测:	3/432
杀软检测:	经检测，该文件安全
MD5:	57f5ff3230be79d521a36d29881567e0
SHA1:	1dcbd71a091347f5404e0ab868[illegible]e01c[illegible]1d0d2c8
SHA256:	462c236919e9984facf305211afda1a6e1f77521c57[illegible]ebc9[illegible]d182f2056b04

分析结果严重性

高危	中危	信息	安全	关注
0	9	1	0	0

四大组件信息

Activity组件：8个，其中export的有：1个
Service组件：3个，其中export的有：1个
Receiver组件：2个，其中export的有：0个
Provider组件：3个，其中export的有：1个

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=IL, ST=IL, L=TLV, O=Rachip, OU=Rachip, CN=Michal
签名算法: rsassa_pkcs1v15
有效期自: 2020-01-12 10:30:03+00:00
有效期至: 2047-05-30 10:30:03+00:00
发行人: C=IL, ST=IL, L=TLV, O=Rachip, OU=Rachip, CN=Michal
序列号: 0x728a5d0b
哈希算法: sha256
证书MD5: 4e58f4f1d2ed508b169b7936a00f01ab
证书SHA1: c622dbfee79dd6aae67da9a910916a92a66e4355
证书SHA256: 21d5cf952808dfddddac44da8f17fc9eb9120e2c1e7e72e7bda3c5a09c11cba7
证书SHA512:
bdbc8eb34e5a4358f763de7d8672affd55b8e8ebc3aa8402d17760284b77a391af08e84d93777b9c47c4d5cf5273e864497b166e72e9f0d9402e67d177f791c9

公钥算法: rsa
密钥长度: 2048
指纹: 0f9ca744d1680bbbb2d2ddc1df00feb2e047b7fe3fd7e79434d1f994aa6c67c9
找到 1 个唯一证书

应用权限

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.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粗略的经纬度信息，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.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.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
android.permission.USE_CREDENTIALS	危险	使用帐户的身份验证凭据	允许应用程序请求身份验证标记。
android.permission.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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。
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。
get.way.com.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
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。
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。

可浏览的Activity组件

ACTIVITY	INTENT

com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.get.way.com,

网络通信安全

序号	范围	严重级别	描述

证书安全分析

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。
4	Content Provider (com.facebook.FacebookContentProvider) 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。
5	Activity (com.facebook.CustomTabActivity) 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	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。

安全漏洞检测

高危: **0** | 警告: **2** | 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	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
3	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

敏感权限分析

类型	匹配	权限
恶意软件常用权限	5/30	android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.GET_ACCOUNTS android.permission.RECORD_AUDIO android.permission.READ_PHONE_STATE
其它常用权限	3/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVIC

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。

域名检测

域名	状态	中国境内	位置信息
fb.gg	安全	否	**IP地址:** 20.190.190.195 **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

www.paypal.com	安全	否	**IP地址:** 20.190.190.195 **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
login.yahoo.com	安全	否	**IP地址:** 20.190.190.195 **国家:** 美利坚合众国 **地区:** 纽约 **城市:** 纽约市 **纬度:** 40.731323 **经度:** -73.990089 **查看:** Google 地图
facebook.com	安全	否	**IP地址:** 20.190.190.195 **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.
graph.s	安全	否	No Geolocation information available.
www.linkedin.com	安全	否	**IP地址:** 20.190.190.195 **国家:** 美利坚合众国 **地区:** 华盛顿 **城市:** 雷德蒙 **纬度:** 47.682899 **经度:** -122.120903 **查看:** Google 地图
twitter.com	安全	否	**IP地址:** 104.244.42.65 **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
login.live.com	安全	否	**IP地址:** 20.190.190.195 **国家:** 美利坚合众国 **地区:** 亚利桑那州 **城市:** 凤凰 **纬度:** 33.448231 **经度:** -112.074051 **查看:** Google 地图

URL链接分析

URL信息	源码文件

• http://stackoverflow.com/questions/3561493/is-there-a-regexp-escape-function-in-javascript • http://stackoverflow.com/questions/181348/instantiating-a-javascript-object-by-calling-prototype-constructor-apply • https://github.com/dordille/moment-isoduration/blob/master/moment.isoduration.js • https://github.com/marceljuenemann/angular-drag-and-drop-lists • https://getway.io/gw/envs/dev2/admin/api/ • https://github.com/moment/moment/issues/1423 • https://www.googletagmanager.com/gtag/js?id=UA-188514276-1 • https://logi-way.com/SubDomain/getway/_gw2aws/gw/envs/dev2-24and26versions/admin/web/ • https://waze.com/ul?ll= • https://logi-way.com/SubDomain/getway/_gw2aws/gw/envs/dev2/admin/api/ • https://logi-way.com/SubDomain/getway/_gw2aws/gw/envs/dev2-24and26versions/admin/api/ • https://github.com/marceljuenemann/angular-drag-and-drop-lists/wiki/Data-Transfer-Design • https://logi-way.com/SubDomain/getway/dev4/admin/api/logApp.php?log= • https://logi-way.com/SubDomain/getway/_gw2aws/gw/envs/dev2/admin/web/ • http://momentjs.com/guides/ • https://cdnjs.cloudflare.com/ajax/libs/angular-material/1.0.4/angular-material.js • https://stackoverflow.com/a/14384091/217866 • http://jsperf.com/b64tests • http://getbootstrap.com • https://getway.logi-way.com/tools/kj2SDsdfGDShJ45FG45.php • https://maxcdn.bootstrapcdn.com/bootstrap/3.4.1/js/bootstrap.min.js • https://github.com/fatlinesofcode/ngDraggable • https://fontawesome.com • https://stackoverflow.com/a/8935649/217866 • https://github.com/moment/moment/issues/2166 • http://getwaywebsite-env.eba-t5smsp7q.us-east-2.elasticbeanstalk.com/gw/envs/dev2/admin/web/ • https://waze.to/?q= • https://www.facebook.com/tr?id=205557051432545&ev=PageView • https://waze.com/ul?q= • https://raw.githubusercontent.com/jakearchibald/es6-promise/master/LICENSE • https://getway.io/gw/envs/dev2/admin/web/ • http://getwaywebsite-env.eba-t5smsp7q.us-east-2.elasticbeanstalk.com/gw/envs/dev2/admin/api/ • http://maps.apple.com/maps?saddr=Current • https://github.com/moment/moment/pull/1871 • https://waze.com/?q= • https://github.com/vskosp/vsGoogleAutocomplete • https://connect.facebook.net/en_US/fbevents.js • https://logi-way.com/SubDomain/getway/dev4/admin/web/ • https://github.com/googlei18n/libphonenumber/blob/master/resources/ShortNumberMetadata.xml • https://cdnjs.cloudflare.com/ajax/libs/angular-material/1.0.4/angular-material.css • https://logi-way.com/SubDomain/getway/dev4/admin/api/ • https://github.com/moment/moment/issues/2978 • https://fontawesome.com/license/free • https://waze.com • https://getway.io/gw/envs/dev2/privacy.html • https://maxcdn.bootstrapcdn.com/bootstrap/3.4.1/css/bootstrap.min.css • https://github.com/behdad/region-flags/tree/gh-pages/png • https://cdnjs.cloudflare.com/ajax/libs/angular.js/1.5.3/angular.min.js • https://waze.to • https://github.com/jackocnr/intl-tel-input.git	启研引擎-A

• https://facebook.com • https://accounts.google.com • https://fb.gg/me/media_asset/ • https://www.linkedin.com • https://fb.gg/me/community/ • https://login.yahoo.com • https://graph-video.%s • https://plus.google.com/ • https://facebook.com/device?user_code=%1$s&qr=1 • https://www.facebook.com/.well-known/oauth/openid/keys/ • http://play.google.com/store/apps/details?id=com.facebook.orca • https://www.paypal.com • https://graph.%s • https://www.facebook.com • https://fb.gg/me/friendfinder/ • https://accounts.google.com/o/oauth2/revoke?token= • https://twitter.com • https://.facebook.com • https://login.live.com	自研引擎-S

第三方SDK

SDK名称	开发者	描述信息
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。
Google Sign-In	Google	提供使用 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。
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。
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。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design) .

追踪器

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

密钥凭证

可能的密钥
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
9b8f518b086098de3d77736f9458a3d2f6f95a37
cc2751449a350f668590264ed76692694a80308a
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
c56fb7d591ba6704df047fd98f535372fea00211
8a3c4b262d721acd49a4bf97d5213199c86fa2b9

GooglePlay应用信息

标题: GetWay-路线规划

评分: 3.65 **安装:** 100,000+ **价格:** 0 **Android版本支持:** **分类:** 地图和导航 **Play Store URL:** get.way.com

开发者信息: Logi Way, Logi+Way, 130 Yoseftal St Zfat, https://getway.io, optimalwaysllc@gmail.com,

发布日期: 2020年3月22日 **隐私政策:** Privacy link

关于此应用:

添加停留点列表，设置起点和终点，其他时间限制，剩下的一切都将自动完成。 使用GetWay应用程序可减少20%的路上时间，让您更快到家。 如何使用GetWay路线规划应用程序来规划路线？ 在GetWay路线规划应用程序中设置起点和终点。 添加停留点，然后GetWay路线规划应用程序将处理剩下的流程。应用程序将根据您提供的停留点，为您的旅行找到最快和最有效的路线。 GetWay路线规划应用程序对一日游有用吗？ 使用GetWay路线规划应用程序将帮助您更快地完成您的一日游。一旦您设计好路线，只需点击一下，就能轻松访问您完成任务所需的任何地址和额外信息。 GetWay路线规划应用程序是否也是当天预订？ GetWay路线规划应用程序的多停留点路线规划为您路线中安排的所有停靠点提供大致的到达时间。如果您未能在预定时间抵达，它将重新计算您其余的时间安排，以便在预定的时间窗口内到达每一站。 GetWay路线规划应用程序是否取代了Google地图或Waze？ 不。在规划好路线后，您可以使用您最喜欢的导航应用程序前往每个目的地。 GetWay路线规划应用程序与您的首选导航应用程序集成，旨在与导航程序一起使用，而不是取代它。 为什么使用GetWay路线规划应用程序进行路线规划？ 通过寻找更短和更有效的路径来完成所有的路线，运输路线用户每天可节省几个小时。

免责声明及风险提示: