MOBSF

ANDROID STATIC ANALYSIS REPORT

Vivian (2.1.7)

File Name:	com.nursefly.NurseFlyMobile_29156.apk
Package Name:	com.nursefly.NurseFlyMobile
Scan Date:	Sept. 1, 2025, 3:04 a.m.
App Security Score:	40/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	12/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	17	2	0	1

FILE INFORMATION

File Name: com.nursefly.NurseFlyMobile_29156.apk
Size: 64.49MB
MD5: 0d8060cc592b378248dbc570b9914427
SHA1: 635df53f5a3f0952784e8a3ef1580643dd305cff
SHA256: 9a890c07b8074f63e8e96f514234d07c5d01b8d61757cf22f7071897bebe68f3

APP INFORMATION

App Name: Vivian
Package Name: com.nursefly.NurseFlyMobile
Main Activity: com.nursefly.NurseFlyMobile.MainActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 2.1.7
Android Version Code: 29156

APP COMPONENTS

Activities: 31
Services: 20
Receivers: 22
Providers: 13
Exported Activities: 3
Exported Services: 3
Exported Receivers: 5
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-04-16 19:20:21+00:00
Valid To: 2048-04-16 19:20:21+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x68a5c5982dac7c1477281d8303a30c3459181cd3
Hash Algorithm: sha256
md5: 8a196bef63cea5af4242dfdb12d85c70
sha1: cdee24ec787ae524d9e0a452ad367544f2fd17da
sha256: f79bc39178ce4677cd4b45e2704f27fbe5e8009d95f4afd0849d4592e9c3cb57
sha512: 9ebf5cf062e43a11b6774b6333e607b0d833c9829844998094696c06e44a32058f92c420483514c8f308d35fc8b3541d8d5573ae83c3532440cb633d0cf1a704
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 53bb172c39b21495c5cb1987c0e73826e7ef1514326be8142be378476c072496
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.nursefly.NurseFlyMobile.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.samsung.android.mapsagent.permission.READ_APP_INFO	unknown	Unknown permission	Unknown permission from android reference
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	unknown	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
0d8060cc592b378248dbc570b9914427.apk	FINDINGS: Anti-VM Code — DETAILS: possible VM check

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>classes10.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check
Build.BOARD check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible Build.SERIAL check
Build.TAGS check
SIM operator check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
network operator name check
ro.kernel.qemu check
possible VM check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>classes6.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes7.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check network operator name check ro.kernel.qemu check possible VM check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>dexlib 2.x</td></tr></table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes8.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
network operator name check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>classes9.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT

ACTIVITY	INTENT
com.nursefly.NurseFlyMobile.MainActivity	Schemes: vh.app://, nursefly://, https://, Hosts: vivian.onelink.me, ablink.news.vivian.com, ablink.mail.vivian.com, vivianhealth.app, vivian.com, www.vivian.com, Path Patterns: /cna/travel/*, /social-work/travel/*, /allied-health/sterile-processing-technician/travel/*, /allied-health/behavioral-health-tech/travel/*, /browse-jobs/landing, /browse-jobs/landing/, /p/landing/*, /*,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.nursefly.NurseFlyMobile,

NETWORK SECURITY

HIGH: **1** | WARNING: **0** | INFO: **0** | SECURE: **0**

NO	SCOPE	SEVERITY	DESCRIPTION
1	nursefly.com www.nursefly.com https://www.nursefly.com	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **0** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: 2 | WARNING: 12 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	App has a Network Security Configuration [android:networkSecurityConfig=@xml/react_native_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
4	Service (com.nursefly.NurseFlyMobile.MainMessagingService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Broadcast Receiver (com.intercom.reactnative.RNIntercomPushBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Broadcast Receiver (io.invertase.firebase.messaging.ReactNativeFirebaseMessagingReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
7	TaskAffinity is set for activity (com.braze.push.NotificationTrampolineActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
8	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
9	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
10	Activity (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Activity (com.google.firebase.auth.internal.RecaptchaActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
13	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
14	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
15	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: **0** | WARNING: **3** | INFO: **1** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/appsflyer/reactnative/RNAppsFlyerConstants.java com/braze/Constants.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/mapbox/maps/plugin/animation/MapAnimationOwnerRegistry.java com/microsoft/codepush/react/CodePushConstants.java com/nimbusds/jose/HeaderParameterNames.java com/nimbusds/jose/jwk/JWKParameterNames.java com/reactnativecommunity/asyncstorage/next/StorageSupplierKt.java io/sentry/SpanDataConvention.java
2	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/fullstory/util/Log.java fsimpl/C0226db.java fsimpl/bA.java fsimpl/dY.java fsimpl/eQ.java
3	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/appsflyer/internal/AFa1vSDK.java com/appsflyer/internal/AFi1fSDK.java
4	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	fsimpl/C0297z.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	me/leolin/shortcutbadger/impl/EverythingMeHomeBadger.java me/leolin/shortcutbadger/impl/HuaweiHomeBadger.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java
00162	Create InetSocketAddress object and connecting to it	socket	org/kaazing/gateway/client/transport/ws/BridgeSocketImpl.java
00163	Create new Socket and connecting to it	socket	org/kaazing/gateway/client/transport/ws/BridgeSocketImpl.java
00013	Read file and put it into a stream	file	bo/app/wc0.java io/sentry/util/FileUtils.java
00012	Read data and put it into a buffer stream	file	io/sentry/util/FileUtils.java
00096	Connect to a URL and set request method	command network	fsimpl/C0271eu.java
00109	Connect to a URL and get the response code	network command	fsimpl/C0271eu.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	me/leolin/shortcutbadger/impl/SonyHomeBadger.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://nursefly-app.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/794315648211/namespaces/firebase:fetch?key=AIzaSyCitcLf6sboIASpCGEEG77_WVNhovPOr0M is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'developerMessage': '{ "bannerText": "We\'re sorry, Vivian is undergoing maintenance for about an hour. We\'ll be back soon!", "buttonText": "OK", "redirectURL": "/", "showBanner": false }', 'hideSamsungKeyboardWarningBanner': 'false', 'minAppVersion': '2.0.79', 'minAppVersionDaysToMuteWarn': '1', 'minAppVersionForce': '-5', 'minAppVersionForceBody': 'An update is required to continue receiving the best experience and latest features', 'minAppVersionForceTitle': 'App update required', 'minAppVersionWarn': '', 'minAppVersionWarnBody': 'Keep the Vivian app up to date for the best experience and the latest features', 'minAppVersionWarnTitle': 'App update available', 'number_of_messages_to_trigger_app_review': '5', 'remoteBanner': '{"displayBanner":false,"body":"We\'re sorry, our servers are temporarily down. Please check back soon.","actionTitle":"App is temporarily down","action":null,"style":{"backgroundColor":"#EA8023","color":"white"}}'}, 'state': 'UPDATE', 'templateVersion': '44'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.VIBRATE, android.permission.CAMERA, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.WAKE_LOCK, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	4/44	com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
www.mapbox.com	ok	**IP:** 199.232.196.143 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
docs.mapbox.com	ok	**IP:** 18.238.96.51 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
nursefly-app.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
sapp.s	ok	No Geolocation information available.

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12

TRACKER	CATEGORIES	URL
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 Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105
Microsoft Visual Studio App Center Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/243
Microsoft Visual Studio App Center Crashes	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/238
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447
fullstory	Analytics	https://reports.exodus-privacy.eu.org/trackers/415

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"CodePushDeploymentKey" : "rA9heysO3fsqiX_Zd5yVuK94VzizGRNy2wh5S"

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"com_braze_api_key" : "92be6f10-e2b5-4603-ae80-012294de3a91"
"com_braze_firebase_cloud_messaging_sender_id" : "794315648211"
"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"
"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"
"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"
"facebook_client_token" : "d65ff544aa979b113e964c14c05f84b7"
"firebase_database_url" : "https://nursefly-app.firebaseio.com"
"google_api_key" : "AIzaSyCitcLf6sboIASpCGEEG77_WVNhovPOr0M"
"google_crash_reporting_api_key" : "AIzaSyCitcLf6sboIASpCGEEG77_WVNhovPOr0M"

PLAYSTORE INFORMATION

Title: Vivian - Find Healthcare Jobs

Score: 4.595092 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.nursefly.NurseFlyMobile

Developer Details: Vivian Health, 7336544802500200355, None, https://www.vivian.com/, founders@nursefly.com,

Release Date: Apr 16, 2018 **Privacy Policy:** Privacy link

Description:

At Vivian, we ensure your next step is a step forward. That’s why we built a jobs marketplace that serves healthcare professionals first. Built on intelligent matching, transparent information and the widest selection of job opportunities, over 1.9 million healthcare professionals turn to Vivian to find their perfect job. Create One Reusable Profile Create a specialized universal profile you can use just like a healthcare resume/CV to quickly and easily apply to healthcare employers nationwide for travel nursing jobs, travel allied health jobs or any type of staff, local contract or per diem healthcare positions. Know What We Know As the leading and largest marketplace for nursing and other healthcare jobs, we have access to an unprecedented amount of unbiased, objective information. From detailed job postings to concrete salary ranges to authentic employer reviews and more, we share what we know with you. Explore Your Options Vivian connects all types of healthcare workers to all types of healthcare jobs. Our marketplace features more than 100 specialties spanning nursing, therapy and allied health jobs, with per diem, staff, local contract and travel positions at top providers nationwide. We’ll show you every job that meets your ideal job criteria. Forget About Endless Calls Plus, endless text messages and emails. With Vivian, you can keep all your applications and messages in one place. Receive instant notifications when a job matches your current needs through our AI job matching and connect with employers right away through our real-time chat. Earn Rewards as a VIP Since launching in 2022, the Vivian VIP program has helped tens of thousands of healthcare professionals get hired. Vivian VIPs enjoy first alerts for preferred travel jobs, boosted credibility and faster responses from recruiters. They can also earn up to $1,550 in financial rewards just for doing what they’re already doing — finding a job on Vivian. Why Download the Vivian App? Join our community of over 1.9 Million incredible healthcare professionals. Vivian has facilitated over 8 Million Job Applications! Get access to trusted health facilities and travel nurse agencies, such as AMN, Cross Country, SSM Health, Honor Health, Host Healthcare, MedPro and many more. Rated 4.5 stars by thousands of healthcare professionals: “I don't have to search dozens of job boards. I added my specialty and the recruiters come to me! One Vivian profile, and I'm done.” Cynthia P. ED - RN, Tampa, FL

SCAN LOGS

Timestamp	Event	Error
2025-09-01 03:04:39	Generating Hashes	OK
2025-09-01 03:04:39	Extracting APK	OK
2025-09-01 03:04:39	Unzipping	OK
2025-09-01 03:04:39	Parsing APK with androguard	OK

2025-09-01 03:04:40	Extracting APK features using aapt/aapt2	OK
2025-09-01 03:04:40	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 03:04:42	Parsing AndroidManifest.xml	OK
2025-09-01 03:04:42	Extracting Manifest Data	OK
2025-09-01 03:04:42	Manifest Analysis Started	OK
2025-09-01 03:04:44	Reading Network Security config from react_native_config.xml	OK
2025-09-01 03:04:44	Parsing Network Security config	OK
2025-09-01 03:04:44	Performing Static Analysis on: Vivian (com.nursefly.NurseFlyMobile)	OK
2025-09-01 03:04:46	Fetching Details from Play Store: com.nursefly.NurseFlyMobile	OK
2025-09-01 03:04:47	Checking for Malware Permissions	OK

2025-09-01 03:04:47	Fetching icon path	OK
2025-09-01 03:04:47	Library Binary Analysis Started	OK
2025-09-01 03:04:47	Reading Code Signing Certificate	OK
2025-09-01 03:04:48	Running APKiD 2.1.5	OK
2025-09-01 03:04:57	Detecting Trackers	OK
2025-09-01 03:05:05	Decompiling APK to Java with JADX	OK
2025-09-01 03:45:35	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/0d8060cc592b378248dbc570b9914427/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/0d8060cc592b378248dbc570b9914427/0d8060cc592b378248dbc570b9914427.apk'], 999.9999803006649)
2025-09-01 03:45:35	Converting DEX to Smali	OK
2025-09-01 03:45:35	Code Analysis Started on - java_source	OK
2025-09-01 03:45:42	Android SBOM Analysis Completed	OK

2025-09-01 03:47:17	Android SAST Completed	OK
2025-09-01 03:47:17	Android API Analysis Started	OK
2025-09-01 03:47:28	Android API Analysis Completed	OK
2025-09-01 03:47:28	Android Permission Mapping Started	OK
2025-09-01 03:47:39	Android Permission Mapping Completed	OK
2025-09-01 03:47:40	Android Behaviour Analysis Started	OK
2025-09-01 03:47:52	Android Behaviour Analysis Completed	OK
2025-09-01 03:47:52	Extracting Emails and URLs from Source Code	OK
2025-09-01 03:47:53	Email and URL Extraction Completed	OK
2025-09-01 03:47:53	Extracting String data from APK	OK
2025-09-01 03:47:53	Extracting String data from Code	OK

2025-09-01 03:47:53	Extracting String values and entropies from Code	OK
2025-09-01 03:47:55	Performing Malware check on extracted domains	OK
2025-09-01 03:47:57	Saving to Database	OK

Report Generated by - MobSF v4.4.0

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.