ANDROID STATIC ANALYSIS REPORT

ShelterApp (2.0.11)

File Name:	ShelterApp.apk
Package Name:	org.strappd
Scan Date:	Nov. 17, 2024, 8:26 p.m.
App Security Score:	48/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	5/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	15	2	1	1

FILE INFORMATION

File Name: ShelterApp.apk
Size: 7.04MB
MD5: 4f85e351587f6076506f66b2e6aa81f1
SHA1: 0613224b5687564044ce2933ce4ebc1ac4472a27
SHA256: b4ebbc7779a3cb098edc85344f7d67f40d45bbad1539ac8ea88222d26f7a387a

APP INFORMATION

App Name: ShelterApp
Package Name: org.strappd
Main Activity: org.strappd.MainActivity
Target SDK: 33
Min SDK: 21
Max SDK:
Android Version Name: 2.0.11

Android Version Code: 20011

APP COMPONENTS

Activities: 7
Services: 7
Receivers: 5
Providers: 4
Exported Activities: 3
Exported Services: 2
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
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: 2018-01-02 18:54:22+00:00
Valid To: 2048-01-02 18:54:22+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x828baf26effd4a58bb47bef2216bdd662f7036ab
Hash Algorithm: sha256
md5: 55cf27a5728da62d79f01713ea9ecd91
sha1: d7e774ab51fcd541789ae2ec429a38abf28bfe02
sha256: efeec86b51841e83d6ea5be3389b6f51f6f3bd1ea700c8b16246258d13dd304b
sha512: 55f89c6eb3c070280cb4ca8a022f67e5fd3489db8c1f910e8c8102261184dfa01e133f1d56fe23dc845e94c5a32588892cda439626a15ad7d1107d2b46c295ba
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 1337545d829fe3911f83199cfeda413e4a41e16b5c2753d6a2c04b42b5a234be
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.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.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
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.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

FILE	DETAILS	
	FINDINGS	DETAILS
classes.dex	Anti-VM Code	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
	Compiler	r8

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.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>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
org.strappd.MainActivity	Schemes: shelter://, Hosts: Auth,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.org.strappd,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

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

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **8** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21]	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	Activity (com.facebook.react.devsupport.DevSettingsActivity) 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.
3	Activity (com.facebook.FacebookActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Service (io.invertase.firebase.messaging.RNFirebaseMessagingService) 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.
5	Broadcast Receiver (com.learnium.RNDeviceInfo.RNDeviceReceiver) 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	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.
7	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.
8	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
9	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [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: **5** | INFO: **1** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				bolts/MeasurementEvent.java co/apptailor/googlesignin/PromiseWrapper.java co/apptailor/googlesignin/RNGoogleSigninModule.java com/agontuk/RNFusedLocation/RNFusedLocationModule.java com/agontuk/RNFusedLocation/SingleLocationUpdate.java com/airbnb/android/react/maps/FileUtil.java com/imagepicker/utils/MediaUtils.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/RNInstallReferrerClient.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java com/lugg/ReactNativeConfig/ReactNativeConfigModule.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/reactnativecommunity/webview/RNCWebViewManager.java com/reactnativecommunity/webview/RNCWebViewModule.java com/swmansion/gesturehandler/react/RNGestureHandlerRootHelper.java com/swmansion/gesturehandler/react/RNGestureHandlerRootView.java io/invertase/firebase/RNFirebaseModule.java io/invertase/firebase/Utils.java io/invertase/firebase/admob/RNFirebaseAdMob.java io/invertase/firebase/analytics/RNFirebaseAnalytics.java io/invertase/firebase/auth/RNFirebaseAuth.java io/invertase/firebase/config/RNFirebaseRemoteConfig.java io/invertase/firebase/database/RNFirebaseDatabase.java io/invertase/firebase/database/RNFirebaseDatabaseReference.java io/invertase/firebase/database/RNFirebaseDatabaseUtils.java io/invertase/firebase/fabric/crashlytics/RNFirebaseCrashlytics.java io/invertase/firebase/firestore/FirestoreSerialize.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/invertase/firebase/firestore/RNFirebaseFirestore.java io/invertase/firebase/firestore/RNFirebaseFirestoreCollectionReference.java io/invertase/firebase/firestore/RNFirebaseFirestoreDocumentReference.java io/invertase/firebase/functions/RNFirebaseFunctions.java io/invertase/firebase/instanceid/RNFirebaseInstanceId.java io/invertase/firebase/links/RNFirebaseLinks.java io/invertase/firebase/messaging/RNFirebaseMessaging.java io/invertase/firebase/messaging/RNFirebaseMessagingService.java io/invertase/firebase/notifications/DisplayNotificationTask.java io/invertase/firebase/notifications/RNFirebaseNotificationManager.java io/invertase/firebase/notifications/RNFirebaseNotifications.java io/invertase/firebase/notifications/RNFirebaseNotificationsRebootReceiver.java io/invertase/firebase/perf/RNFirebasePerformance.java io/invertase/firebase/storage/RNFirebaseStorage.java me/leolin/shortcutbadger/ShortcutBadger.java
2	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	bolts/WebViewAppLinkResolver.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	bolts/MeasurementEvent.java io/invertase/firebase/functions/RNFirebaseFunctions.java io/invertase/firebase/notifications/RNFirebaseNotificationManager.java io/invertase/firebase/notifications/RNFirebaseNotifications.java org/strappd/BuildConfig.java
4	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/imagepicker/utils/MediaUtils.java com/imagepicker/utils/RealPathUtil.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnativecommunity/webview/RNCWebViewModule.java io/invertase/firebase/storage/RNFirebaseStorage.java
5	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	com/airbnb/android/react/maps/AirMapModule.java com/airbnb/android/react/maps/FileUtil.java com/reactnativecommunity/webview/RNCWebViewModule.java
6	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00123	Save the response to JSON after connecting to the remote server	network command	bolts/WebViewAppLinkResolver.java
00089	Connect to a URL and receive input stream from the server	command network	bolts/WebViewAppLinkResolver.java io/invertase/firebase/notifications/DisplayNotificationTask.java
00030	Connect to the remote server through the given URL	network	bolts/WebViewAppLinkResolver.java io/invertase/firebase/notifications/DisplayNotificationTask.java
00109	Connect to a URL and get the response code	network command	bolts/WebViewAppLinkResolver.java
00094	Connect to a URL and read data from it	command network	bolts/WebViewAppLinkResolver.java
00108	Read the input stream from given URL	network command	bolts/WebViewAppLinkResolver.java
00091	Retrieve data from broadcast	collection	io/invertase/firebase/notifications/RNFirebaseBackgroundNotificationActionReceiver.java io/invertase/firebase/notifications/RNFirebaseNotifications.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	bolts/AppLinkNavigation.java bolts/AppLinks.java bolts/MeasurementEvent.java io/invertase/firebase/links/RNFirebaseLinks.java io/invertase/firebase/notifications/RNFirebaseNotificationManager.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java
00022	Open a file from given absolute path of the file	file	com/imagepicker/ImagePickerModule.java com/imagepicker/media/ImageConfig.java com/imagepicker/utils/MediaUtils.java com/oblador/vectoricons/VectorIconsModule.java io/invertase/firebase/storage/RNFirebaseStorage.java
00013	Read file and put it into a stream	file	com/airbnb/android/react/maps/AirMapLocalTile.java com/airbnb/android/react/maps/FileUtil.java com/imagepicker/ImagePickerModule.java com/imagepicker/utils/MediaUtils.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java okio/Okio.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	bolts/AppLinkNavigation.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	bolts/AppLinkNavigation.java bolts/MeasurementEvent.java com/airbnb/android/react/maps/AirMapMarker.java com/airbnb/android/react/maps/ImageReader.java com/imagepicker/utils/RealPathUtil.java io/invertase/firebase/notifications/RNFirebaseNotificationManager.java me/leolin/shortcutbadger/impl/EverythingMeHomeBadger.java me/leolin/shortcutbadger/impl/HuaweiHomeBadger.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java
00189	Get the content of a SMS message	sms	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00188	Get the address of a SMS message	sms	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00191	Get messages in the SMS inbox	sms	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00200	Query data from the contact list	collection contact	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00187	Query a URI and check the result	collection sms calllog calendar	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00201	Query data from the call log	collection calllog	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00078	Get the network operator name	collection telephony	com/learnium/RNDeviceInfo/RNDeviceModule.java
00038	Query the phone number	collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00130	Get the current WIFI information	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00134	Get the current WiFi IP address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceModule.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java
00192	Get messages in the SMS inbox	sms	com/imagepicker/utils/RealPathUtil.java io/invertase/firebase/notifications/RNFirebaseNotificationManager.java
00175	Get notification manager and cancel notifications	notification	io/invertase/firebase/notifications/RNFirebaseNotificationManager.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/airbnb/android/react/maps/ImageUtil.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://shelterapp-1573928197721.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/972668199767/namespaces/firebase:fetch?key=AIzaSyC63EJ9w6OUC4QwtsNb9PyrNOQqr54xbkg. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.INTERNET, android.permission.CAMERA, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_FINE_LOCATION, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.VIBRATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK
Other Common Permissions	2/44	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
api.shelter.app	ok	**IP:** 44.227.24.210 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
shelterapp-1573928197721.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66

TRACKER	CATEGORIES	URL
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Places		https://reports.exodus-privacy.eu.org/trackers/69
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"FCM_TOKEN" : "@fcmToken_shelter"
"GOOGLE_MAPS_APIKEY" : "AIzaSyDg2iZZy3zugO2Uo-brrUcfRv6khyQSoKo"
"INSTAGRAM_APP_SECRET" : "2e6309f18710a8f2b14acbcf3e000545"
"TWITTER_COMSUMER_KEY" : "GkOT1u6XJjPt5eQOWsQOiBTdS"
"TWITTER_CONSUMER_SECRET" : "z9OpBbQHCEtLEvyHP9tyZuFx03Xr1mSn8dQDfkX5l3tj1hUW1U"
"WWW_MOBILE_API_URL" : "https://api.shelter.app"
"firebase_database_url" : "https://shelterapp-1573928197721.firebaseio.com"
"google_api_key" : "AIzaSyC63EJ9w6OUC4QwtsNb9PyrNOQqr54xbkg"

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyC63EJ9w6OUC4QwtsNb9PyrNOQqr54xbkg"
B3EEABB8EE11C2BE770B684D95219ECB
9b8f518b086098de3d77736f9458a3d2f6f95a37
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
2e6309f18710a8f2b14acbcf3e000545
cc2751449a350f668590264ed76692694a80308a
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
5e8f16062ea3cd2c4a0d547876baa6f38cabf625
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
z9OpBbQHCEtLEvyHP9tyZuFx03Xr1mSn8dQDfkX5l3tj1hUW1U
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc

PLAYSTORE INFORMATION

Title: Homeless Resources-Shelter App

Score: 3.8790324 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Books & Reference **Play Store URL:** org.strappd

Developer Details: Shelter App Team, 7058593917292214574, None, https://strappd.org, shelterappinfo@gmail.com,

Release Date: Jan 2, 2018 **Privacy Policy:** Privacy link

Description:

Shelter App, Inc. is an All-volunteer Non-Profit Organization that helps Homeless and At-risk Youth connect to services using a mobile app where they can find Food, Shelter, Health, Resources and Work. Our Shelter App(formerly Strappd) has resources for Youth across US and resources for everyone in Colorado and in following Counties/Cities: Los Angeles County, King County(Seattle), Multnomah County(Portland), Orange County, San Bernardino County, Riverside County, San Francisco County, Santa Clara County(San Jose), Alameda County(Oakland), San Diego County and El Paso County. Shelter App is an AI Powered Chatbot that connects at-risk youth to services like Youth Drop-in Centers, Homeless & Run Away Youth Shelters, LGBT Advocacy and Support Groups, After School Programs, Crisis or Hot lines, Food Banks, Soup Kitchens, Food Pantries, Transitional Housing, Domestic Violence Shelters, Pet Shelters, Rent/Utility Assistance, Affordable Housing Options, Free or Low-cost Medical & Dental Clinics, Mental Health Centers, HIV/STI Testing Centers, Syringe Exchange Programs, Clothing Resources, Free Legal clinics, Hygiene Services, Showers, Restrooms, Homeless and Low-income Family Resources, Education & Employment Assistance Services, Job Training Programs, Life Skills Training, Mentorship & many more resources for Homeless and People in Need. App Users can switch from List View to Map View and can filter services that are just open from the side menu. Users can click on any service to get details like contact info, transit directions and schedule for that service. Flag button on Home Screen will help you connect to the App Admin or Service Provider for that resource. Users can click on Kudos button to show appreciation for the services they like. If you want to mark any service for future reference, click on the star icon in service detail page to add them to My Favorites. If you are doing community service and interested in listing your service, you can add/manage a service by signing up in the app. You can also update the number of beds available for shelters that you manage. All details entered by the service providers will take some time to get approved before getting published in the app. If you have any questions or see information that is not up to date, please report changes using Give Feedback in side menu. Download our app to find Homeless resources close to you.

SCAN LOGS

Timestamp	Event	Error
2024-11-17 20:26:13	Generating Hashes	OK
2024-11-17 20:26:13	Extracting APK	OK
2024-11-17 20:26:13	Unzipping	OK

2024-11-17 20:26:13	Getting Hardcoded Certificates/Keystores	OK
2024-11-17 20:26:13	Parsing APK with androguard	OK
2024-11-17 20:26:14	Parsing AndroidManifest.xml	OK
2024-11-17 20:26:14	Extracting Manifest Data	OK
2024-11-17 20:26:14	Performing Static Analysis on: ShelterApp (org.strappd)	OK
2024-11-17 20:26:14	Fetching Details from Play Store: org.strappd	OK
2024-11-17 20:26:15	Manifest Analysis Started	OK
2024-11-17 20:26:15	Checking for Malware Permissions	OK
2024-11-17 20:26:15	Fetching icon path	OK
2024-11-17 20:26:15	Library Binary Analysis Started	OK

2024-11-17 20:26:15	Reading Code Signing Certificate	OK
2024-11-17 20:26:15	Running APKiD 2.1.5	OK
2024-11-17 20:26:16	Detecting Trackers	OK
2024-11-17 20:26:17	Decompiling APK to Java with JADX	OK
2024-11-17 20:26:24	Converting DEX to Smali	OK
2024-11-17 20:26:24	Code Analysis Started on - java_source	OK
2024-11-17 20:26:25	Android SAST Completed	OK
2024-11-17 20:26:25	Android API Analysis Started	OK
2024-11-17 20:26:25	Android API Analysis Completed	OK
2024-11-17 20:26:25	Android Permission Mapping Started	OK
2024-11-17 20:26:27	Android Permission Mapping Completed	OK

2024-11-17 20:26:28	Email and URL Extraction Completed	OK
2024-11-17 20:26:28	Android Behaviour Analysis Started	OK
2024-11-17 20:26:28	Android Behaviour Analysis Completed	OK
2024-11-17 20:26:28	Extracting String data from APK	OK
2024-11-17 20:26:28	Extracting String data from Code	OK
2024-11-17 20:26:28	Extracting String values and entropies from Code	OK
2024-11-17 20:26:30	Performing Malware check on extracted domains	OK
2024-11-17 20:26:30	Saving to Database	OK

Report Generated by - MobSF v4.1.9

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.