ANDROID STATIC ANALYSIS REPORT

LazyFit (2.0.40)

File Name:	com.mejordailytracker.app_124.apk
Package Name:	com.mejordailytracker.app
Scan Date:	Aug. 31, 2025, 3:59 a.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	15	2	2	1

FILE INFORMATION

File Name: com.mejordailytracker.app_124.apk
Size: 141.79MB
MD5: 8bb23edc6eaac418bd50948af2bf5bfd
SHA1: 71f87dd2526de4f6aa1452e618a291a8e34080ec
SHA256: b385c0beac8319c8b3d136d5b46b794183a6814dbf0bc3e436ff096237ac50c4

APP INFORMATION

App Name: LazyFit
Package Name: com.mejordailytracker.app
Main Activity: com.glority.android.picturexx.splash.SplashActivity
Target SDK: 34
Min SDK: 29
Max SDK:
Android Version Name: 2.0.40

Android Version Code: 124

▦ APP COMPONENTS

Activities: 31
Services: 17
Receivers: 12
Providers: 4
Exported Activities: 1
Exported Services: 2
Exported Receivers: 3
Exported Providers: 0

✹ CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: False
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: 2021-12-27 11:39:49+00:00
Valid To: 2051-12-27 11:39:49+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xd9d11446224ac4f9323483544b4929342e7c628e
Hash Algorithm: sha256
md5: e84528cf246088b00f4ada28b5f880bb
sha1: 1eb0f999226085e6a204bc81ec310b70072841a4
sha256: 27123dc1a891b10b45a7364983c542cd540021e642b59dafdc941a72f26f7970
sha512: 2a2144713ba7e491dede6f6d3cc12fd3e3550775d8c35f97398459056bad5108710e2051abb2d8e564301a29a4402d1e6d7f16eac6aa05656e0e252b0c991653
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 91ae94bc41481da8d06da710be76b51c99a46a8a4dea312ca3bf4217089d8740
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.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.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
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.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>8bb23edc6eaac418bd50948af2bf5bfd.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
possible VM check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes10.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

<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>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table></td></tr>
<tr><td>classes3.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table></td></tr>
<tr><td>classes4.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</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>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes6.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes7.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check
Build.BOARD check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes8.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.BOARD check
Build.TAGS check
subscriber ID check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes9.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.glority.android.picturexx.view.deeplink.DeeplinkLauncherActivity	Schemes: lazyfit://, Hosts: dl, Paths: /delete,
com.glority.android.picturexx.splash.SplashActivity	Schemes: lazyfit://, Hosts: dl, Paths: /delete,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

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: **1** | WARNING: **6** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Activity (com.glority.android.picturexx.view.deeplink.DeeplinkLauncherActivity) 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
3	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.
4	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.
5	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
6	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.
7	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: **1** | WARNING: **7** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES

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/amazonaws/auth/policy/conditions/ConditionFactory.java com/amazonaws/auth/policy/conditions/S3ConditionFactory.java com/amazonaws/mobileconnectors/s3/transferutility/TransferTable.java com/amazonaws/services/s3/Headers.java com/amazonaws/services/s3/model/S3ObjectSummary.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/glority/android/netimageadapter/glidecode/DataCacheKey.java com/glority/android/picturexx/settings/logevents/SettingsLogEvents.java com/glority/android/ui/base/LocaleManager.java com/glority/app/BuildConfig.java com/mux/stats/sdk/core/model/CustomerPlayerData.java com/mux/stats/sdk/core/model/SessionTag.java io/reactivex/internal/schedulers/SchedulerPoolFactory.java
				com/amazonaws/logging/AndroidLog.java com/amazonaws/logging/ConsoleLog.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SingletonConnectivityReceiver.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/glority/android/core/utils/device/DeviceIdFactory.java com/glority/android/guide/view/cardview/YcCardViewApi21.java com/glority/android/guide/view/cardview

NO	ISSUE	SEVERITY	STANDARDS	FILES
				/YcRoundRectDrawable.java com/glority/android/guide/view/cardview/YcRoundRectDrawableWithShadow.java com/glority/android/international/firebase/MyJobService.java com/glority/android/picturexx/util/PulseDetector.java com/glority/android/ui/base/LocaleManager.java com/glority/base/utils/crop/CropCoverDrawable.java com/glority/base/utils/crop/CropHelper.java com/glority/base/widget/FixedWebView.java com/glority/base/widget/webview/FixedWebView.java com/glority/utils/app/AppUtils.java com/glority/utils/device/NetworkUtils.java com/glority/utils/stability/CrashHelper.java com/glority/utils/ui/ViewUtils.java com/glority/widget/imagepager/GlImageViewTouch.java com/glority/widget/skeleton/ViewReplacer.java
3	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/amazonaws/mobileconnectors/s3/transferutility/TransferTable.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/glority/imagepicker/utils/FileUtils.java com/glority/utils/stability/CrashHelper.java com/glority/utils/store/FileUtils.java com/glority/utils/store/PathUtils.java com/glority/utils/store/SandboxUtils.java
5	The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	com/glority/encrypt/AESCrypt.java
6	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/glority/base/utils/SHAHelper.java
7	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/glority/base/utils/StringUtil.java
8	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/airbnb/lottie/network/NetworkCache.java com/amazonaws/services/s3/internal/MD5DigestCalculatingInputStream.java com/glority/android/networkconfig/util/Md5Utils.java com/glority/network/util/Md5Utils.java com/glority/utils/data/EncryptUtils.java com/glority/utils/store/FileUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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/mux/stats/sdk/core/util/UUID.java
10	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/glority/utils/device/NetworkUtils.java
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/glority/utils/device/DeviceUtils.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/airbnb/lottie/network/NetworkCache.java com/amazonaws/auth/PropertiesCredentials.java com/glority/base/utils/crop/CropHelper.java com/glority/utils/stability/CrashHelper.java com/glority/utils/store/FileUtils.java com/glority/utils/store/PathUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/airbnb/lottie/network/NetworkCache.java com/amazonaws/auth/PropertiesCredentials.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/glority/base/utils/SHAHelper.java com/glority/utils/data/EncryptUtils.java com/glority/utils/store/FileUtils.java com/glority/utils/store/IOUtils.java
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java
00030	Connect to the remote server through the given URL	network	com/adjust/sdk/AdjustLinkResolution.java com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/glority/utils/store/FileUtils.java
00189	Get the content of a SMS message	sms	com/glority/utils/store/SandboxUtils.java
00188	Get the address of a SMS message	sms	com/glority/utils/store/SandboxUtils.java
00200	Query data from the contact list	collection contact	com/glority/utils/store/SandboxUtils.java
00201	Query data from the call log	collection calllog	com/glority/utils/store/SandboxUtils.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/glority/utils/store/SandboxUtils.java
00202	Make a phone call	control	com/glority/utils/app/IntentUtils.java
00203	Put a phone number into an intent	control	com/glority/utils/app/IntentUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/glority/utils/app/IntentUtils.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/glority/utils/app/IntentUtils.java
00074	Get IMSI and the ISO country code	collection telephony	com/glority/utils/device/DeviceUtils.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/glority/utils/device/DeviceUtils.java
00146	Get the network operator name and IMSI	telephony collection	com/glority/utils/device/DeviceUtils.java
00117	Get the IMSI and network operator name	telephony collection	com/glority/utils/device/DeviceUtils.java
00084	Get the ISO country code and IMSI	collection telephony	com/glority/utils/device/DeviceUtils.java
00192	Get messages in the SMS inbox	sms	com/glority/utils/store/FileUtils.java
00012	Read data and put it into a buffer stream	file	com/glority/utils/store/FileUtils.java
00109	Connect to a URL and get the response code	network command	com/glority/utils/store/FileUtils.java
00191	Get messages in the SMS inbox	sms	com/glority/utils/store/FileUtils.java
00094	Connect to a URL and read data from it	command network	com/glority/utils/store/FileUtils.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/83501635683/namespaces/firebase:fetch?key=AIzaSyB0Yn2uJN0QUNGuYubpUgDlwcakFa_U45M. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.VIBRATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	4/44	android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, 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
app.eu.adjust.com	ok	**IP:** 185.151.204.60 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
gdpr.adjust.world	ok	**IP:** 185.151.204.40 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
gdpr.tr.adjust.com	ok	**IP:** 195.244.54.44 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
app.adjust.com	ok	**IP:** 185.151.204.13 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
subscription.tr.adjust.com	ok	**IP:** 195.244.54.7 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map
gdpr.adjust.com	ok	**IP:** 185.151.204.50 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
subscription.adjust.world	ok	**IP:** 185.151.204.44 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 142.250.188.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
gdpr.eu.adjust.com	ok	**IP:** 185.151.204.60 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
subscription.eu.adjust.com	ok	**IP:** 185.151.204.60 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
gdpr.us.adjust.com	ok	**IP:** 185.151.204.70 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
subscription.adjust.net.in	ok	**IP:** 185.151.204.34 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
app.adjust.world	ok	**IP:** 185.151.204.43 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
gw.mejorai.com	ok	**IP:** 35.168.161.93 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
subscription.us.adjust.com	ok	**IP:** 185.151.204.70 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
app.tr.adjust.com	ok	**IP:** 195.244.54.44 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map
gdpr.adjust.net.in	ok	**IP:** 185.151.204.32 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
app-service.mejorai.com	ok	**IP:** 54.146.251.94 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
app.us.adjust.com	ok	**IP:** 185.151.204.70 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
subscription.adjust.com	ok	**IP:** 185.151.204.52 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
acs.amazonaws.com	ok	No Geolocation information available.
www.amazon.com	ok	**IP:** 23.222.206.109 **Country:** United States of America **Region:** Minnesota **City:** Minneapolis **Latitude:** 44.979969 **Longitude:** -93.263840 **View:** Google Map
app.adjust.net.in	ok	**IP:** 185.151.204.31 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

EMAILS

EMAIL	FILE
support@thevisionext.com	com/glority/app/BuildConfig.java

TRACKERS

TRACKER	CATEGORIES	URL
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"google_api_key" : "AIzaSyB0Yn2uJN0QUNGuYubpUgDlwcakFa_U45M"
"google_crash_reporting_api_key" : "AIzaSyB0Yn2uJN0QUNGuYubpUgDlwcakFa_U45M"

POSSIBLE SECRETS
"google_maps_key" : "AIzaSyAUbrOoI5AZqjQyxYKznRcCCFm43Ek9Py0"
1bd2462077e211eb8cfbc3eedc210400

PLAYSTORE INFORMATION

Title: LazyFit: Chair Yoga & Pilates

Score: 4.4527473 **Installs:** 5,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.mejordailytracker.app

Developer Details: Next Vision Limited, Next+Vision+Limited, None, https://mejorai.com/, support@mejorai.com,

Release Date: Apr 30, 2022 **Privacy Policy:** Privacy link

Description:

Do you wanna be lazy and fit at the same time? Want to lose weight? Need to gain muscle? Have no equipment? LazyFit is perfect for you. LazyFit, your scientifically designed virtual fitness coach, keeps you motivated on your fitness journey. Join our 28-day challenge for your fitness goal. Explore 28-day chair exercises, bed workouts, yoga, wall pilates, somatic exercises, and more. LazyFit provides personalized recommendations based on your preferences, lifestyle, and fitness goals. Whether you want to lose weight, gain muscle, or adopt a healthier lifestyle, LazyFit is here for you. Incorporating Somatic Exercises, LazyFit adds mindfulness to your routine. Whether you're a senior seeking chair fitness or a yoga beginner, LazyFit caters to all your needs. LazyFit provides Customized Support for Your Body. LazyFit is designed to offer targeted assistance for your body's needs during workouts. When you're focusing on rehabilitation, have certain areas of vulnerability, or simply want to prevent injury, LazyFit offers tailored exercises and movements. By targeting specific muscle groups and joints while reducing strain on areas, LazyFit helps you exercise with confidence and peace of mind, knowing that your body is being looked after. With LazyFit, you can enjoy the benefits of physical activity while minimizing health risks and promoting a safer workout experience. Enjoy flexible workouts anywhere with LazyFit. Our diverse at-home sets require no equipment. Benefit from a personalized approach to speed up your weight loss or muscle gain goals. Key Features: - Workout Coach: Personalized workout plans for faster results - From Beginner to Advanced: Fitness exercises for all levels - 28-Day Challenge: Jumpstart your fitness journey with LazyFit - Target Training: Focus on specific areas - Wall Pilates Workouts: Pilates with wall-based exercises - Belly Exercises for Women: Focused belly fat workouts for a toned core - Somatic Exercises: Mindful workouts for well-being and mental health - Chair Yoga for seniors: Added comfort with chair workouts - Bed Exercises: Get fit while being lazy in bed with fun and no pain - Yoga: Enhance flexibility and balance with yoga - Senior Fitness: Tailored exercises for seniors to maintain health - Stretching Routine: Enhance flexibility; Reduce stress and prevent lower back pain - Daily Progress Tracker: Track your everyday progress to stay on track - Health & Fitness Tips: Explore resources to keep you on the right track. Join LazyFit's 28-day challenge in achieving your fitness goals. LazyFit, your fitness companion, offers yoga, chair workouts for seniors, wall pilates, bed workouts, somatic exercises, targeted training, and personalized exercises. Join the community of thousands that have transformed themselves with LazyFit. Start your holistic fitness experience today. Lazy, loud, and proud, let's get fit together! Terms of Use: https://app-service.lazyfit.ai/static/user_agreement_20230320.html Privacy Policy: https://app-service.lazyfit.ai/static/privacy_policy_20230817.html Contact us: support@lazyfit.ai

SCAN LOGS

Timestamp	Event	Error
2025-08-31 03:59:08	Generating Hashes	OK
2025-08-31 03:59:08	Extracting APK	OK
2025-08-31 03:59:08	Unzipping	OK
2025-08-31 03:59:09	Parsing APK with androguard	OK
2025-08-31 03:59:11	Extracting APK features using aapt/aapt2	OK
2025-08-31 03:59:11	Getting Hardcoded Certificates/Keystores	OK
2025-08-31 03:59:14	Parsing AndroidManifest.xml	OK
2025-08-31 03:59:14	Extracting Manifest Data	OK
2025-08-31 03:59:14	Manifest Analysis Started	OK

2025-08-31 03:59:14	Performing Static Analysis on: LazyFit (com.mejordailytracker.app)	OK
2025-08-31 03:59:16	Fetching Details from Play Store: com.mejordailytracker.app	OK
2025-08-31 03:59:17	Checking for Malware Permissions	OK
2025-08-31 03:59:17	Fetching icon path	OK
2025-08-31 03:59:17	Library Binary Analysis Started	OK
2025-08-31 03:59:17	Reading Code Signing Certificate	OK
2025-08-31 03:59:18	Running APKiD 2.1.5	OK
2025-08-31 03:59:23	Detecting Trackers	OK
2025-08-31 03:59:32	Decompiling APK to Java with JADX	OK

2025-08-31 04:19:41	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/8bb23edc6eaac418bd50948af2bf5bfd/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/8bb23edc6eaac418bd50948af2bf5bfd/8bb23edc6eaac418bd50948af2bf5bfd.apk'], 999.9999847784638)
2025-08-31 04:19:41	Converting DEX to Smali	OK
2025-08-31 04:19:41	Code Analysis Started on - java_source	OK
2025-08-31 04:19:47	Android SBOM Analysis Completed	OK
2025-08-31 04:20:02	Android SAST Completed	OK
2025-08-31 04:20:02	Android API Analysis Started	OK
2025-08-31 04:20:07	Android API Analysis Completed	OK
2025-08-31 04:20:08	Android Permission Mapping Started	OK
2025-08-31 04:20:14	Android Permission Mapping Completed	OK
2025-08-31 04:20:14	Android Behaviour Analysis Started	OK

2025-08-31 04:20:22	Android Behaviour Analysis Completed	OK
2025-08-31 04:20:22	Extracting Emails and URLs from Source Code	OK
2025-08-31 04:20:27	Email and URL Extraction Completed	OK
2025-08-31 04:20:27	Extracting String data from APK	OK
2025-08-31 04:20:27	Extracting String data from Code	OK
2025-08-31 04:20:27	Extracting String values and entropies from Code	OK
2025-08-31 04:20:31	Performing Malware check on extracted domains	OK
2025-08-31 04:20:35	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.