MOBSF

ANDROID STATIC ANALYSIS REPORT

12Steps (1.1.7)

File Name:	12 Steps_ Addiction Recovery_1.1.7_APKPure.xapk
Package Name:	com.twelve_steps.twelve_steps
Scan Date:	Nov. 29, 2024, 4:42 a.m.
App Security Score:	47/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	16	2	2	1

FILE INFORMATION

File Name: 12 Steps_ Addiction Recovery_1.1.7_APKPure.xapk
Size: 10.18MB
MD5: eb267511a5cd53a1a43a626271a4877a
SHA1: 88a9ea656e88022fac9f70cca120057342fde149
SHA256: 05cacd571a52d2e537deacb693bcdd41f975d7f77a57d5d857e1d7e25b7a1f82

APP INFORMATION

App Name: 12Steps
Package Name: com.twelve_steps.twelve_steps
Main Activity: com.twelve_steps.twelve_steps.MainActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 1.1.7

Android Version Code: 196

APP COMPONENTS

Activities: 13
Services: 8
Receivers: 6
Providers: 5
Exported Activities: 3
Exported Services: 1
Exported Receivers: 3
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: 2023-06-09 02:19:14+00:00
Valid To: 2053-06-09 02:19:14+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x25fa55d774baf5c932a5cfd98e9f7d9e30666959
Hash Algorithm: sha256
md5: 5f97fcc2d3517df1963fb55052fc56c2
sha1: abf2e8c11b0751012c65cc26e8df94efabe33e6b
sha256: 832544223d0e6b1bd77fc72a94758b54133f9984f8b0767655a7e9993ae60b29
sha512: ebfdb668413398cd74f6f5bbd3b01f38eb459b42082b61e844ea2c1da80886b2a90d4c2b8a446dd36d441e8dc25f6c43495e528629c7d93d4661f6be66848f6d
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 50a7b167b420281ec8ce429e35d8aeacf4da6f80d247a989ef53aeda66c79beb
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.

PERMISSION	STATUS	INFO	DESCRIPTION
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.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.twelve_steps.twelve_steps.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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

APKID ANALYSIS

FILE	DETAILS

<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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check
ro.hardware 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>dx</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes2.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.HARDWARE check</td></tr><tr><td>Compiler</td><td>dx</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.twelve_steps.twelve_steps.MainActivity	Schemes: https://, Hosts: link.12steps.app, Path Prefixes: /1hlr,
com.aboutyou.dart_packages.sign_in_with_apple.SignInWithAppleCallback	Schemes: signinwithapple://, Paths: callback,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

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: 2 | WARNING: 7 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched 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.

NO	ISSUE	SEVERITY	DESCRIPTION
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	Activity (com.aboutyou.dart_packages.sign_in_with_apple.SignInWithAppleCallback) 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.
4	Broadcast Receiver (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) 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	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.
6	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.

NO	ISSUE	SEVERITY	DESCRIPTION
7	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.
8	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.
9	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: **2** | WARNING: **7** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b1/f.java b1/m.java c4/r.java com/appsflyer/appsflyersdk/AppsflyerSdkPlugin.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1qSDK.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1jSDK.java com/appsflyer/internal/AFf1kSDK.java com/appsflyer/internal/AFg1jSDK.java com/dexterous/flutterlocalnotifications/ActionBroadcastReceiver.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/dexterous/flutterlocalnotifications/ScheduledNotificationReceiver.java com/pichillilorenzo/flutter_inappwebview_android/MyCookieManager.java com/pichillilorenzo/flutter_inappwebview_android/Util.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ChromeCustomTabsActivity.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java com/pichillilorenzo/flutter_inappwebview_android/content_blocker/ContentBlockerHandler.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserActivity.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/pichillilorenzo/flutter_inappwebview_android/service_worker/ServiceWorkerManager.java com/pichillilorenzo/flutter_inappwebview_android/types/WebViewAssetLoaderExt.java com/pichillilorenzo/flutter_inappwebview_android/webview/JavaScriptBridgeInterface.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/DisplayListenerProxy.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/FlutterWebView.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebView.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebViewChromeClient.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebViewClient.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebViewClientCompat.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebViewRenderProcessClient.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InputAwareWebView.java d5/a.java d8/c.java e5/a.java e7/d0.java e7/g.java e7/g0.java e7/i0.java e7/k.java e7/y.java e8/f.java f/d.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	f7/a.java f8/a.java f8/c.java g1/a.java g4/o.java g5/i.java g7/c.java g7/f.java i8/d.java io/flutter/plugins/firebase/crashlytics/n.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundService.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingReceiver.java io/flutter/plugins/firebase/messaging/b.java io/flutter/plugins/firebase/messaging/i.java io/flutter/plugins/webviewflutter/f.java io/flutter/plugins/webviewflutter/o3.java j0/d.java j1/a.java j1/n.java j1/o.java j1/p.java k8/b.java k8/c.java n0/c.java n4/g.java n5/g.java o0/a.java o9/a.java p4/b.java p4/b0.java p4/c0.java p4/d.java p4/k.java p4/u.java p4/w.java p4/y.java p8/d.java q9/e.java r1/k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				r9/i.java s4/a.java s5/a1.java s5/b1.java s5/d0.java s5/e.java s5/g0.java s5/i0.java s5/j1.java s5/k0.java s5/m1.java s5/q0.java s5/u0.java s5/v1.java s5/x0.java s9/a.java s9/d0.java t5/f.java t5/n.java t9/i.java u/c.java u0/a.java u1/a.java u4/a.java u6/b.java v4/n.java v4/o.java v6/c.java v8/b.java w0/q.java w5/g.java x/c.java y0/a.java y0/e.java ya/c.java z5/r.java z7/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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/pichillilorenzo/flutter_inappwebview_android/credential_database/CredentialDatabaseHelper.java h8/e.java y1/m0.java y1/t0.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/AFa1zSDK.java com/appsflyer/internal/AFb1hSDK.java com/appsflyer/internal/AFc1fSDK.java e3/w0.java h3/b.java ja/a.java
4	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	a3/a.java a6/b.java b6/e.java b6/w.java com/appsflyer/appsflyersdk/AppsFlyerConstants.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/dexterous/flutterlocalnotifications/models/NotificationDetails.java com/pichillilorenzo/flutter_inappwebview_android/credential_database/URLCredentialContract.java com/pichillilorenzo/flutter_inappwebview_android/types/ClientCertResponse.java com/pichillilorenzo/flutter_inappwebview_android/types/HttpAuthResponse.java com/pichillilorenzo/flutter_inappwebview_android/types/URLCredential.java s9/c0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	r9/a.java r9/i.java
6	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/appsflyer/internal/AFb1vSDK.java
7	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	j3/a.java
8	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	l3/b.java
9	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	u6/b.java
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	g5/w.java z5/i.java
11	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	k8/c.java m8/b.java u6/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	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	io/flutter/plugin/editing/b.java io/flutter/plugin/platform/d.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	a6/f.java com/appsflyer/internal/AFg1nSDK.java g6/a.java u6/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	a6/f.java b0/m.java b4/d0.java b4/g.java com/appsflyer/internal/AFb1iSDK.java com/appsflyer/internal/AFg1nSDK.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/pichillilorenzo/flutter_inappwebview_android/Util.java e6/e.java ea/k.java ea/m.java g6/a.java u6/c.java z5/a0.java
00009	Put data in cursor to JSON object	file	h8/e.java
00096	Connect to a URL and set request method	command network	b4/s.java com/appsflyer/internal/AFb1uSDK.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java com/pichillilorenzo/flutter_inappwebview_android/Util.java i8/b.java v6/c.java
00123	Save the response to JSON after connecting to the remote server	network command	com/pichillilorenzo/flutter_inappwebview_android/Util.java
00030	Connect to the remote server through the given URL	network	b4/s.java com/appsflyer/internal/AFb1uSDK.java com/pichillilorenzo/flutter_inappwebview_android/Util.java

RULE ID	BEHAVIOUR	LABEL	FILES
00094	Connect to a URL and read data from it	command network	b4/s.java com/pichillilorenzo/flutter_inappwebview_android/Util.java d6/a.java i8/b.java
00091	Retrieve data from broadcast	collection	com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1jSDK.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ActionBroadcastReceiver.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ChromeCustomTabsActivity.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserActivity.java
00089	Connect to a URL and receive input stream from the server	command network	b4/s.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java i8/b.java v6/c.java
00109	Connect to a URL and get the response code	network command	b4/s.java com/appsflyer/internal/AFb1uSDK.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java com/appsflyer/internal/AFf1oSDK.java i8/b.java n4/f.java v6/c.java
00132	Query The ISO country code	telephony collection	c4/m0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/aboutyou/dart_packages/sign_in_with_apple/a.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1cSDK.java com/appsflyer/internal/AFc1jSDK.java com/appsflyer/internal/AFf1sSDK.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ChromeCustomTabsActivity.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ChromeCustomTabsChannelDelegate.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/TrustedWebActivity.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserManager.java j1/a.java j1/n.java j1/p.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java p8/d.java s5/f1.java t9/h.java za/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	b4/d0.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFi1mSDK.java com/appsflyer/internal/AFi1sSDK.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java j1/a.java j1/n.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java me/leolin/shortcutbadger/impl/a.java p8/d.java za/b.java za/c.java za/d.java
00056	Modify voice volume	control	org/webrtc/audio/WebRtcAudioTrack.java org/webrtc/voiceengine/WebRtcAudioTrack.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/aboutyou/dart_packages/sign_in_with_apple/a.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserManager.java j1/a.java j1/n.java j1/p.java t9/h.java
00022	Open a file from given absolute path of the file	file	a6/f.java b0/m.java com/appsflyer/internal/AFg1nSDK.java r9/i.java z8/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFi1oSDK.java me/leolin/shortcutbadger/impl/a.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFi1oSDK.java me/leolin/shortcutbadger/impl/a.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1sSDK.java me/leolin/shortcutbadger/impl/a.java
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFi1mSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1qSDK.java me/leolin/shortcutbadger/impl/a.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFi1oSDK.java me/leolin/shortcutbadger/impl/a.java
00187	Query a URI and check the result	collection sms calllog calendar	me/leolin/shortcutbadger/impl/a.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFi1oSDK.java me/leolin/shortcutbadger/impl/a.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1sSDK.java me/leolin/shortcutbadger/impl/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00161	Perform accessibility service action on accessibility node info	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/c.java u/c.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/AFh1cSDK.java h8/n.java
00108	Read the input stream from given URL	network command	b4/s.java i8/b.java
00199	Stop recording and release recording resources	record	f8/c.java k8/b.java
00198	Initialize the recorder and start recording	record	f8/c.java k8/b.java
00194	Set the audio source (MIC) and recorded file format	record	f8/c.java k8/b.java
00197	Set the audio encoder and initialize the recorder	record	f8/c.java k8/b.java
00196	Set the recorded file format and output path	record file	f8/c.java k8/b.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java u/c.java
00003	Put the compressed bitmap data into JSON object	camera	com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebView.java

RULE ID	BEHAVIOUR	LABEL	FILES
00005	Get absolute path of file and put it to JSON object	file	a6/f.java com/appsflyer/internal/AFg1nSDK.java
00209	Get pixels from the latest rendered image	collection	io/flutter/embedding/android/g.java
00210	Copy pixels from the latest rendered image into a Bitmap	collection	io/flutter/embedding/android/g.java
00028	Read file from assets directory	file	b4/c.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1jSDK.java
00183	Get current camera parameters and change the setting.	camera	org/webrtc/Camera1Session.java
00208	Capture the contents of the device screen	collection screen	org/webrtc/ScreenCapturerAndroid.java
00202	Make a phone call	control	j1/p.java
00203	Put a phone number into an intent	control	j1/p.java
00102	Set the phone speaker on	command	co/daily/daily_flutter/AudioManager.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/681308934040/namespaces/firebase:fetch?key=AIzaSyArkUAumo_Mr8IA1RZib1H141ZL2viocB0. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.RECORD_AUDIO, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK
Other Common Permissions	4/44	android.permission.MODIFY_AUDIO_SETTINGS, 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
play.google.com	ok	**IP:** 216.58.209.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.microsoft.com	ok	**IP:** 13.107.246.45 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
dashif.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebase.google.com	ok	**IP:** 216.58.211.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
issuetracker.google.com	ok	**IP:** 216.58.210.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sattr.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
docs.flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
scdn-ssettings.s	ok	No Geolocation information available.
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sgcdsdk.s	ok	No Geolocation information available.
exoplayer.dev	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
sadrevenue.s	ok	No Geolocation information available.
sars.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
simpression.s	ok	No Geolocation information available.
accounts.google.com	ok	**IP:** 108.177.14.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sonelink.s	ok	No Geolocation information available.
sconversions.s	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.
sdlsdk.s	ok	No Geolocation information available.
svalidate.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
www.example.com	ok	**IP:** 93.184.215.14 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.apple.com	ok	**IP:** 17.253.39.206 **Country:** Sweden **Region:** Stockholms lan **City:** Stockholm **Latitude:** 59.332581 **Longitude:** 18.064899 **View:** Google Map
smonitorsdk.s	ok	No Geolocation information available.
ns.adobe.com	ok	No Geolocation information available.
aomedia.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
developer.android.com	ok	**IP:** 216.58.209.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sapp.s	ok	No Geolocation information available.
sinapps.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
sviap.s	ok	No Geolocation information available.
api.mixpanel.com	ok	**IP:** 35.190.25.25 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
scdn-stestsettings.s	ok	No Geolocation information available.
firebase-settings.crashlytics.com	ok	**IP:** 216.58.210.131 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27

HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AIzaSyArkUAumo_Mr8IA1RZib1H141ZL2viocB0"
"google_crash_reporting_api_key" : "AIzaSyArkUAumo_Mr8IA1RZib1H141ZL2viocB0"
9a04f079-9840-4286-ab92-e65be0885f95
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
af60eb711bd85bc1e4d3e0a462e074eea428a8

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
470fa2b4ae81cd56ecbcda9735803434cec591fa
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
36864200e0eaf5284d884a0e77d31646
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

POSSIBLE SECRETS
115792089210356248762697446949407573530086143415290314195533631308867097853951
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
bae8e37fc83441b16034566b

PLAYSTORE INFORMATION

Title: 12 Steps: Addiction Recovery

Score: 4.9 **Installs:** 10,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.twelve_steps.twelve_steps

Developer Details: OpenRecovery, OpenRecovery, 42 Broadway, Suite 12-580 New York, NY 10004 USA, https://www.12steps.app, support@12steps.app,

Release Date: Aug 11, 2023 **Privacy Policy:** Privacy link

Description:

Welcome to 12 Steps: Addiction Recovery, an AI-powered platform featuring Kai, your personal Recovery Assistant, designed to support your journey through any 12-step program. Kai offers customized, adaptive guidance tailored to your unique path, respecting diverse beliefs and backgrounds in a supportive, ad-free environment. Whether your sponsor is unavailable or you're not ready to share with someone else, Kai is here to listen. Embrace Your Recovery Journey with tools crafted to meet you where you are—from starting out to maintaining long-term progress—ensuring support every step of the way. Key Features: • Kai, Your AI-Powered Recovery Assistant: Chat with Kai about any aspect of your recovery, receiving real-time, personalized support. Kai remembers important details like your sponsor's name and how you refer to your higher power, making your experience truly personal. Use voice interaction for inventories and step work, allowing natural, conversational engagement that helps you navigate challenging moments anytime you need. • Neutral Approach to Literature: Access 12-step content in a neutral style, supportive for any spiritual or religious background. • Personalized Content Recommendations: From account creation, receive tailored content based on your program and current step for relevant guidance from day one. • Steps Support: Access videos, readings, and templates for each step, providing structured tools to help you stay on track. • Customizable Content Feed: Stay motivated with daily inspiration that adapts to your emotions and goals, encouraging new habits and a positive lifestyle. • Accountability and Habit-Building Tools: Manage recurring actions with accountability features that strengthen relationships with sponsors and partners, reinforcing positive habits crucial to your journey. • Extensive Recovery Library: Explore resources like the AA Big Book, Twelve Steps and Twelve Traditions, program-specific prayers, and more to deepen your understanding. • Sobriety Tracking with Daycounts & Milestones: Track multiple day counts for different aspects of your recovery, from your main sobriety date to personal goals. Celebrate achievements privately or with the community. Sharing milestones fosters support in your recovery network, while Kai helps recognize and

celebrate each accomplishment. • Interactive Inventory Templates: Engage in self-reflection with Step 4 and Step 10 templates, addressing patterns and behaviors in a structured way. • Spot Checks: Quickly assess your emotional state with instant spot checks, receiving personalized suggestions to manage everyday challenges. • Dynamic Action Planner: Define your readiness and motivation for change. Kai offers customized daily action suggestions and lets you add personal tasks to support your growth. Supported Programs Include: • AA - Alcoholics Anonymous • ACA - Adult Children of Alcoholics • Al-Anon / Alateen • CA - Cocaine Anonymous • Co-Anon • CoDA - Co-Dependents Anonymous • COSLAA - Co-Sex and Love Addicts Anonymous • DA - Debtors Anonymous • EA - Emotions Anonymous • Gam-Anon / Gam-A-Teen • GA - Gamblers Anonymous • HA - Heroin Anonymous • NA - Narcotics Anonymous • Nar-Anon • OA - Overeaters Anonymous • SA - Sexaholics Anonymous • SAA - Sex Addicts Anonymous • SCA - Sexual Compulsives Anonymous • SLAA - Sex and Love Addicts Anonymous • RA - Rageaholics Anonymous • UA - Underearners Anonymous • WA - Workaholics Anonymous • MA - Marijuana Anonymous • CMA - Crystal Meth Anonymous 12 Steps: Addiction Recovery is your companion on this journey, offering support every step of the way. Join a community where milestones are celebrated, and challenges are met with understanding, empathy, and actionable insights through Kai’s guidance.

SCAN LOGS

Timestamp	Event	Error
2024-11-29 04:42:27	Generating Hashes	OK
2024-11-29 04:42:27	Extracting APK	OK
2024-11-29 04:42:27	Unzipping	OK
2024-11-29 04:42:27	Parsing APK with androguard	OK
2024-11-29 04:42:28	Extracting APK features using aapt/aapt2	OK
2024-11-29 04:42:28	Getting Hardcoded Certificates/Keystores	OK

2024-11-29 04:42:33	Parsing AndroidManifest.xml	OK
2024-11-29 04:42:33	Extracting Manifest Data	OK
2024-11-29 04:42:33	Manifest Analysis Started	OK
2024-11-29 04:42:33	Performing Static Analysis on: 12Steps (com.twelve_steps.twelve_steps)	OK
2024-11-29 04:42:33	Fetching Details from Play Store: com.twelve_steps.twelve_steps	OK
2024-11-29 04:42:33	Checking for Malware Permissions	OK
2024-11-29 04:42:33	Fetching icon path	OK
2024-11-29 04:42:33	Library Binary Analysis Started	OK
2024-11-29 04:42:33	Reading Code Signing Certificate	OK
2024-11-29 04:42:34	Running APKiD 2.1.5	OK
2024-11-29 04:42:38	Detecting Trackers	OK

2024-11-29 04:42:41	Decompiling APK to Java with JADX	OK
2024-11-29 04:43:24	Converting DEX to Smali	OK
2024-11-29 04:43:24	Code Analysis Started on - java_source	OK
2024-11-29 04:43:27	Android SBOM Analysis Completed	OK
2024-11-29 04:44:06	Android SAST Completed	OK
2024-11-29 04:44:06	Android API Analysis Started	OK
2024-11-29 04:44:45	Android API Analysis Completed	OK
2024-11-29 04:44:46	Android Permission Mapping Started	OK
2024-11-29 04:45:21	Android Permission Mapping Completed	OK
2024-11-29 04:45:21	Android Behaviour Analysis Started	OK
2024-11-29 04:45:28	Android Behaviour Analysis Completed	OK

2024-11-29 04:45:28	Extracting Emails and URLs from Source Code	OK
2024-11-29 04:45:32	Email and URL Extraction Completed	OK
2024-11-29 04:45:32	Extracting String data from APK	OK
2024-11-29 04:45:32	Extracting String data from Code	OK
2024-11-29 04:45:32	Extracting String values and entropies from Code	OK
2024-11-29 04:45:35	Performing Malware check on extracted domains	OK
2024-11-29 04:45:37	Saving to Database	OK
2024-11-29 04:47:21	Unzipping	OK
2024-11-29 04:59:06	Unzipping	OK

Report Generated by - MobSF v4.2.8

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.