MOBSF

ANDROID STATIC ANALYSIS REPORT

Finch (3.72.55)

File Name:	com.finch.finch_993.apk
Package Name:	com.finch.finch
Scan Date:	Aug. 29, 2025, 10:15 p.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	21	3	3	2

FILE INFORMATION

File Name: com.finch.finch_993.apk
Size: 111.71MB
MD5: 2b319753a291ab0759e9c870ad2da1c5
SHA1: ff703f78baab422b32978c081347c12581cb18c3
SHA256: 005364a0de56a2315d72d6e10162877d58deb17f9b8edc5595de3086f35cc238

APP INFORMATION

App Name: Finch
Package Name: com.finch.finch
Main Activity: com.finch.finch.MainActivity
Target SDK: 35
Min SDK: 25
Max SDK:
Android Version Name: 3.72.55

Android Version Code: 993

APP COMPONENTS

Activities: 9
Services: 13
Receivers: 12
Providers: 8
Exported Activities: 2
Exported Services: 1
Exported Receivers: 6
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: 2020-08-25 19:15:39+00:00
Valid To: 2050-08-25 19:15:39+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x2cdb49a3d3db76f36f63fb56977d5a6c4418bbb3
Hash Algorithm: sha256
md5: c03507364431c3b26ca7689c3e3977ac
sha1: cedfd7aedf208ab6d6e2ba90f6508dfd8674959f
sha256: 581db964c61c25369a50142a3e96f1c825c37a70c2ddf333214b4be31c955bc7
sha512: 38a124df1737a340c1ea2c822f550e10ff9a74cf03aa64201850441e70b019184439e225eab5b5414dc5c6f3c6e82d561dbba566b4fd8df32d2c44ba90a422ab
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 2fac5f9023d39c761c5c88a7b2ba0173d8e9980e934fda73fbcba5c59bc6cfd7
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.

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.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	normal	enables foreground services for media playback.	Allows a regular application to use Service.startForeground with the type "mediaPlayback".
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
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.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

PERMISSION	STATUS	INFO	DESCRIPTION
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.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.finch.finch.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check Build.TAGS check SIM operator check network operator name check device ID check</td></tr><tr><td>Obfuscator</td><td>Kiwi encrypter</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</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>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
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT

ACTIVITY	INTENT
com.finch.finch.MainActivity	Schemes: http://, https://, Hosts: app.befinch.com/share, app.befinch.com/invite, app.befinch.com/invite_v1, app.befinch.com/invite_v2, app.befinch.com/invite_v3, app.befinch.com/invite_v4, app.befinch.com/invite_v5, app.befinch.com/invite_v6, app.befinch.com/invite_v7,
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: 1 | WARNING: 10 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.1-7.1.2, [minSdk=25]	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	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Broadcast Receiver (com.finch.finch.FinchHomeWidgetProvider) 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.
4	Broadcast Receiver (com.adjust.sdk.AdjustReferrerReceiver) 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.
5	Service (com.ryanheise.audioservice.AudioService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Broadcast Receiver (com.ryanheise.audioservice.MediaButtonReceiver) 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.
7	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.
8	Broadcast Receiver (com.amazon.device.iap.ResponseReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.amazon.inapp.purchasing.Permission.NOTIFY [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.
9	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.
10	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
11	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.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 9 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a5/b.java a8/b.java a9/a.java a9/b.java a9/c.java a9/i.java b5/g.java b5/p.java b5/q.java b6/g.java b8/c.java b9/e.java com/adjust/sdk/Logger.java com/adjust/sdk/flutter/AdjustSdk.java com/amazon/a/a/g/d.java com/amazon/a/a/o/c.java com/amazon/c/a/a/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/amazon/device/drm/LicensingService.java com/amazon/device/drm/a/d/c.java com/amazon/device/iap/PurchasingService.java com/amazon/device/iap/internal/c/e.java com/amazon/device/simplesignin/BroadcastHandler.java com/amazon/device/simplesignin/SimpleSignInService.java com/amazon/device/simplesignin/a/a/c/b.java com/amazon/device/simplesignin/a/c.java com/amazon/device/simplesignin/a/c/b.java com/dexterous/flutterlocalnotifications/ActionBroadcastReceiver.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/dexterous/flutterlocalnotifications/ScheduledNotificationReceiver.java com/finch/finch/FinchHomeWidgetProvider.java com/mr/flutter/plugin/filepicker/b.java com/mr/flutter/plugin/filepicker/c.java com/revenuecat/purchases/common/DefaultLogHandler.java com/revenuecat/purchases/hybridcommon/CommonKt.java com/revenuecat/purchases/hybridcommon/mappers/PurchasesPeriod.java com/revenuecat/purchases_flutter/PurchasesFlutterPlugin.java com/ryanheise/audioservice/AudioService.java com/ryanheise/audioservice/a.java d1/c.java d2/k.java d7/g.java f5/b.java g1/b.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	g2/a.java h0/d.java h6/a.java h8/e.java i5/a.java i6/b.java ic/c.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/sentry/android/core/u.java io/sentry/android/replay/s.java io/sentry/android/replay/v.java io/sentry/flutter/SentryFlutter$updateOptions$24.java io/sentry/flutter/SentryFlutterPlugin.java io/sentry/flutter/SentryFlutterReplayRecorder.java io/sentry/m6.java k5/a.java k6/b1.java k6/d0.java k6/e0.java k6/f0.java k6/f1.java k6/j0.java k6/o0.java k6/p0.java k6/r1.java k6/v0.java k6/w0.java k6/y1.java k8/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ka/a.java kc/a.java kc/b.java l4/r.java l5/a.java l6/f.java l6/n.java la/b.java lc/a.java mb/b.java n5/i.java o6/g.java p4/a.java qa/d.java qc/i.java r0/a.java r1/i.java r6/s.java rc/k.java sa/a.java sc/i.java t0/d.java t4/b.java t4/d.java t4/h.java t4/r.java t4/s.java t4/u.java t4/x.java t4/y.java u/k0.java u0/a.java u4/e0.java u4/f.java u4/q.java u4/u.java u4/z.java u7/w.java u8/a.java u8/e.java ua/b0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ua/d0.java ua/l.java wc/a.java x4/a.java x8/c0.java x8/f0.java x8/g.java x8/h0.java x8/k.java x8/x.java y0/a.java y8/a.java z/c.java z0/a.java z8/c.java za/d.java
	Files may contain hardcoded		CWE: CWE-312: Cleartext Storage of Sensitive Information	com/adjust/sdk/Constants.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/dexterous/flutterlocalnotifications/models/NotificationDetails.java com/revenuecat/purchases/amazon/AmazonBillingKt.java com/revenuecat/purchases/amazon/AmazonCacheKt.java com/revenuecat/purchases/common/BackendKt.java com/revenuecat/purchases/common/BackgroundAwareCallbackCacheKey.java com/revenuecat/purchases/common/caching/DeviceCache.java com/revenuecat/purchases/common/diagnostics/DiagnosticsEntry.java com/revenuecat/purchases/common/diagnostics/DiagnosticsHelper.java com/revenuecat/purchases/common/diagnostics/DiagnosticsTracker.java com/revenuecat/purchases/common/offlineentitlements/ProductEntitlementMappi

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	sensitive information like usernames, passwords, keys etc.	warning	information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	ng.java com/revenuecat/purchases/common/verification/DefaultSignatureVerifier.java
				com/revenuecat/purchases/common/verification/Signature.java com/revenuecat/purchases/common/verification/SigningManager.java com/revenuecat/purchases/strings/ConfigureStrings.java com/revenuecat/purchases/subscriberattributes/SubscriberAttribute.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java io/grpc/internal/m2.java l1/j.java o7/a.java q7/b.java q7/r.java r7/f.java s6/b.java t6/e.java t6/w.java t7/x0.java w8/b.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	k2/m0.java k2/t0.java p7/a3.java p7/z3.java r1/n.java ua/i.java
4	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	a8/b.java com/amazon/a/a/o/b/a.java com/revenuecat/purchases/common/UtilsKt.java fb/b.java io/sentry/util/u.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	a9/c.java com/adjust/sdk/Util.java com/amazon/a/a/b/b.java com/amazon/a/a/i/b.java com/amazon/a/a/l/c.java dd/e.java dd/g.java io/grpc/internal/c0.java io/grpc/internal/e0.java io/grpc/internal/z1.java j$/util/concurrent/ThreadLocalRandom.java p2/q1.java p8/d.java q3/r0.java ra/d.java t3/b.java u7/h0.java vd/a.java vd/b.java wd/a.java xc/i.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/amazon/a/a/o/b/a.java ef/e.java ef/f.java
7	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/mr/flutter/plugin/filepicker/b.java com/mr/flutter/plugin/filepicker/c.java io/sentry/android/core/r0.java qc/a.java qc/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	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	a8/c.java u/q.java
9	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	la/b.java v3/a.java
10	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/d.java io/flutter/plugin/platform/f.java sa/a.java
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/n.java n5/w.java r6/i.java
12	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/amazon/device/drm/LicensingService.java com/amazon/device/iap/PurchasingService.java
13	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/n.java
14	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	t7/m.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/amazon/a/a/b/b.java com/mr/flutter/plugin/filepicker/c.java io/sentry/android/core/cache/b.java io/sentry/android/core/r0.java io/sentry/android/core/z.java io/sentry/android/replay/capture/f.java io/sentry/android/replay/g.java io/sentry/cache/b.java io/sentry/cache/c.java io/sentry/cache/e.java io/sentry/flutter/SentryFlutterReplayRecorder.java io/sentry/k5.java io/sentry/p.java io/sentry/q2.java io/sentry/s2.java io/sentry/w.java l0/m.java qc/i.java s6/f.java u/q.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	a8/c.java com/adjust/sdk/PreinstallUtil.java com/amazon/c/a/a/c.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/mr/flutter/plugin/filepicker/c.java com/revenuecat/purchases/common/FileHelper.java io/sentry/android/core/SentryPerformanceProvider.java io/sentry/android/replay/g.java io/sentry/cache/b.java io/sentry/cache/c.java io/sentry/cache/e.java io/sentry/config/e.java io/sentry/q2.java io/sentry/s2.java io/sentry/util/e.java io/sentry/w.java k4/g.java k4/h0.java l0/m.java pd/j.java r0/a.java r6/b0.java s6/f.java u/q.java w6/e.java y6/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/adjust/sdk/ActivityHandler.java com/adjust/sdk/PreinstallUtil.java com/amazon/a/a/i/a.java com/amazon/a/a/i/g.java com/amazon/device/iap/internal/a/a.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/mr/flutter/plugin/filepicker/b.java com/ryanheise/audioservice/AudioService.java d7/g.java gc/h.java k6/z0.java sa/a.java sc/h.java ta/a.java za/d.java
00091	Retrieve data from broadcast	collection	com/amazon/device/drm/a/d/c.java com/amazon/device/iap/internal/c/e.java com/amazon/device/simplesignin/a/c/b.java
00012	Read data and put it into a buffer stream	file	com/amazon/c/a/a/c.java com/mr/flutter/plugin/filepicker/c.java io/sentry/cache/b.java io/sentry/cache/e.java io/sentry/config/e.java io/sentry/q2.java io/sentry/util/e.java io/sentry/w.java r0/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	com/adjust/sdk/AdjustLinkResolution.java io/sentry/SpotlightIntegration.java io/sentry/transport/o.java k4/s.java
00189	Get the content of a SMS message	sms	k1/c.java z1/b.java
00188	Get the address of a SMS message	sms	k1/c.java z1/b.java
00200	Query data from the contact list	collection contact	k1/c.java z1/b.java
00187	Query a URI and check the result	collection sms calllog calendar	k1/c.java z1/b.java
00201	Query data from the call log	collection calllog	k1/c.java z1/b.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	z1/b.java
00016	Get location info of the device and put it to JSON object	location collection	r1/g.java
00162	Create InetSocketAddress object and connecting to it	socket	ef/a.java ef/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00163	Create new Socket and connecting to it	socket	com/adjust/sdk/network/ActivityPackageSender.java ef/a.java ef/f.java
00014	Read file into a stream and put it into a JSON object	file	a8/c.java s6/f.java y6/a.java
00005	Get absolute path of file and put it to JSON object	file	s6/f.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	sa/a.java sc/h.java ta/a.java
00089	Connect to a URL and receive input stream from the server	command network	b8/c.java com/revenuecat/purchases/common/HTTPClient.java io/sentry/SpotlightIntegration.java io/sentry/transport/o.java k4/s.java r1/l.java
00109	Connect to a URL and get the response code	network command	b8/c.java com/revenuecat/purchases/common/HTTPClient.java io/sentry/SpotlightIntegration.java io/sentry/transport/o.java k4/s.java p4/a.java r1/l.java
00078	Get the network operator name	collection telephony	r1/p.java

RULE ID	BEHAVIOUR	LABEL	FILES
00137	Get last known location of the device	location collection	r1/p.java
00115	Get last known location of the device	collection location	r1/p.java
00132	Query The ISO country code	telephony collection	l4/p0.java ma/a.java r1/p.java
00036	Get resource file from res/raw directory	reflection	com/adjust/sdk/ActivityHandler.java com/adjust/sdk/InstallReferrerHuawei.java com/adjust/sdk/a.java com/amazon/a/a/i/g.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/finch/finch/FinchHomeWidgetProvider.java com/ryanheise/audioservice/AudioService.java k4/h0.java sa/a.java za/d.java
00102	Set the phone speaker on	command	pa/l.java
00056	Modify voice volume	control	pa/l.java
00126	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	k1/c.java
00094	Connect to a URL and read data from it	command network	k4/s.java v6/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	b8/c.java com/revenuecat/purchases/common/HTTPClient.java io/sentry/SpotlightIntegration.java io/sentry/transport/o.java k4/s.java
00009	Put data in cursor to JSON object	file	r1/n.java
00004	Get filename and put it to JSON object	file collection	r1/n.java
00191	Get messages in the SMS inbox	sms	com/adjust/sdk/a.java
00092	Send broadcast	command	lb/b.java
00161	Perform accessibility service action on accessibility node info	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/e.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java
00108	Read the input stream from given URL	network command	k4/s.java
00209	Get pixels from the latest rendered image	collection	io/flutter/embedding/android/n.java
00210	Copy pixels from the latest rendered image into a Bitmap	collection	io/flutter/embedding/android/n.java

RULE ID	BEHAVIOUR	LABEL	FILES
00028	Read file from assets directory	file	k4/c.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://finch-6819a.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/391357715085/namespaces/firebase:fetch?key=AIzaSyCFd6UB42tM36WnMD9vwGIKruv6VuxePmg. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	10/25	android.permission.INTERNET, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.READ_CONTACTS, android.permission.CAMERA, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	5/44	com.google.android.gms.permission.AD_ID, android.permission.WRITE_CONTACTS, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION
app.adjust.cn	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
app.adjust.cn	ok	**IP:** 47.104.30.117 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
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:** 195.244.54.7 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.revenuecat.com	ok	**IP:** 52.21.13.22 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
app.adjust.com	ok	**IP:** 185.151.204.11 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
api.eu.amplitude.com	ok	**IP:** 52.58.123.64 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
issuetracker.google.com	ok	**IP:** 64.233.177.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
subscription.tr.adjust.com	ok	**IP:** 195.244.54.6 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map
gdpr.adjust.com	ok	**IP:** 185.151.204.51 **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
play.google.com	ok	**IP:** 172.253.124.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
default.url	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
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
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
firebase.google.com	ok	**IP:** 74.125.136.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developer.android.com	ok	**IP:** 64.233.176.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **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
rev.cat	ok	**IP:** 52.72.49.79 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **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
finch-6819a.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
bit.ly	ok	**IP:** 67.199.248.10 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **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

DOMAIN	STATUS	GEOLOCATION
app.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
api-diagnostics.revenuecat.com	ok	**IP:** 54.160.110.226 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
api2.amplitude.com	ok	**IP:** 44.238.64.219 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
developer.apple.com	ok	**IP:** 17.253.83.143 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
app.tr.adjust.com	ok	**IP:** 195.244.54.5 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map
gdpr.adjust.net.in	ok	**IP:** 185.151.204.30 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
www.twitter.com	ok	**IP:** 172.66.0.227 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **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
ns.adobe.com	ok	No Geolocation information available.
api-paywalls.revenuecat.com	ok	**IP:** 54.160.110.226 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
schemas.microsoft.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 142.250.9.94 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
errors.rev.cat	ok	**IP:** 67.199.248.13 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
docs.revenuecat.com	ok	**IP:** 18.238.109.64 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **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
regionconfig.eu.amplitude.com	ok	**IP:** 18.238.96.4 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebasestorage.googleapis.com	ok	**IP:** 173.194.219.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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
www.amazon.com	ok	**IP:** 18.238.90.46 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
regionconfig.amplitude.com	ok	**IP:** 18.155.173.77 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
console.firebase.google.com	ok	**IP:** 64.233.176.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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
u0013android@android.com0 u0013android@android.com	u4/p.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
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://finch-6819a.firebaseio.com"
"google_api_key" : "AIzaSyCFd6UB42tM36WnMD9vwGIKruv6VuxePmg"
"google_crash_reporting_api_key" : "AIzaSyCFd6UB42tM36WnMD9vwGIKruv6VuxePmg"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166438125740282911150571 51

POSSIBLE SECRETS
470fa2b4ae81cd56ecbcda9735803434cec591fa
VGhpcyBpcyB0aGUga2V5IGZvciBhIHNlY3VyZSBzdG9yYWdlIEFFUyBLZXkK
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMlM=
9a04f079-9840-4286-ab92-e65be0885f95
30820268308201d102044a9c4610300d06092a864886f70d0101040500307a310b3009060355040613025553310b3009060355040813024341311230100603550407130950616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b130846616365626f6f6b311d301b06035504031314466163656265626f6f6b20436f72706f726174696f6e3020170d3039303833313231353231365a180f32303530303932353231353231365a307a310b3009060355040613025553310b3009060355040813024341311230100603550407130950616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b13084661636562656f6f6b311d301b06035504031314466616365626f6f6b20436f72706f726174696f6e30819f300d06092a864886f70d010101050003818d0030818902818100c207d51df8eb8c97d93ba0c8c1002c928fab00dc1b42fca5e66e99cc3023ed2d214d822bc59e8e35ddcf5f44c7ae8ade50d7e0c434f500e6c131f4a2834f987fc46406115de2018ebbb0d5a3c261bd97581ccfef76afc7135a6d59e8855ecd7eacc8f8737e794c60a761c536b72b11fac8e603f5da1a2d54aa103b8a13c0dbc10203010001300d06092a864886f70d010104050003818100 5ee9be8bcbb250648d3b741290a82a1c9dc2e76a0af2f2228f1d9f9c4007529c446a70175c5a900d5141812866db46be6559e2141616483998211f4a673149fb2232a10d247663b26a9031e15f84bc1c74d141ff98a02d76f85b2c8ab2571b6469b232d8e768a7f7ca04f7abe4a775615916c07940656b58717457b42bd928a2
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBhIHNlY3VyZSBzdG9yYWdlCg
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

POSSIBLE SECRETS
e2719d58-a985-b3c9-781a-b030af78d30e
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
115792089210356248762697446949407573530086143415290314195533631308867097853951
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: Finch: Self-Care Pet

Score: 4.9122515 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.finch.finch

Developer Details: Finch Care Public Benefit Corporation, 5628861420212947727, None, https://finchcare.com/, support@befinch.com,

Release Date: May 11, 2021 **Privacy Policy:** Privacy link

Description:

Meet your new self-care best friend! Finch is a self-care pet app that helps you feel prepared and positive, one day at a time. Take care of your pet by taking care of yourself! Choose from a wide variety of daily self-care exercises personalized for you. BEST DAILY SELF-CARE TRACKER Is self-care a chore? Struggling with habits, self-love, or depression? Self-care finally feels rewarding, lightweight, and fun with Finch. Complete quick self-care exercises to grow your pet, earn rewards, and improve mental health! People who struggle with mood journaling, habits, and depression found it easier to be mindful with their self-care pet in Finch! EASY DAILY CHECK INS ✏ • Start mornings with quick mood checks and energize your pet to go exploring! Choose from various mindful habits from goal tracking and mood journaling to mindful breathing exercises and quizzes! • End days in moments of gratitude with your self-care pet where they'll return from adventures to share stories with you! Recognize positive moments and grow your self-love. MINDFUL HABITS Finch is the fun self-care tracker to hit goals and sustain healthy habits! Build mental resilience against stress, anxiety, and depression. Strengthen your mental health by increasing self-love and gratitude. • Habit Tracker: set goals and celebrate wins for healthy habits. • Mood Journal: guided mood journal to clear the mind, track important moments, and practice self-love. • Breathing: guided breathing to calm nerves, increase focus, energize your mind, and sleep better. • Quizzes: understand your mental health with quizzes for anxiety, depression, body image appreciation, and more. • Mood Tracker: quick mood checks with mood trends to understand what has been lifting you up or bringing you down. • Quotes: motivational quotes to lift your mood and gain new perspective. • Insights: get insights on your mental health from combined analytics on your mood journaling, tags, goal tracker, and quizzes. SAY HI • TikTok: https://www.tiktok.com/@finchcare • Discord: https://discord.gg/finchfam • Instagram: https://www.instagram.com/finchcare/ • Facebook: https://facebook.com/groups/finchfam • Email: support@befinch.com

SCAN LOGS

Timestamp	Event	Error
2025-08-29 22:15:46	Generating Hashes	OK
2025-08-29 22:15:47	Extracting APK	OK
2025-08-29 22:15:47	Unzipping	OK
2025-08-29 22:15:49	Parsing APK with androguard	OK
2025-08-29 22:15:50	Extracting APK features using aapt/aapt2	OK

2025-08-29 22:15:50	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 22:15:55	Parsing AndroidManifest.xml	OK
2025-08-29 22:15:55	Extracting Manifest Data	OK
2025-08-29 22:15:55	Manifest Analysis Started	OK
2025-08-29 22:15:55	Performing Static Analysis on: Finch (com.finch.finch)	OK
2025-08-29 22:15:55	Fetching Details from Play Store: com.finch.finch	OK
2025-08-29 22:15:56	Checking for Malware Permissions	OK
2025-08-29 22:15:56	Fetching icon path	OK
2025-08-29 22:15:56	Library Binary Analysis Started	OK
2025-08-29 22:15:56	Reading Code Signing Certificate	OK
2025-08-29 22:15:57	Running APKiD 2.1.5	OK

2025-08-29 22:16:07	Detecting Trackers	OK
2025-08-29 22:16:09	Decompiling APK to Java with JADX	OK
2025-08-29 22:16:24	Converting DEX to Smali	OK
2025-08-29 22:16:24	Code Analysis Started on - java_source	OK
2025-08-29 22:16:27	Android SBOM Analysis Completed	OK
2025-08-29 22:16:35	Android SAST Completed	OK
2025-08-29 22:16:35	Android API Analysis Started	OK
2025-08-29 22:16:42	Android API Analysis Completed	OK
2025-08-29 22:16:42	Android Permission Mapping Started	OK
2025-08-29 22:16:48	Android Permission Mapping Completed	OK
2025-08-29 22:16:48	Android Behaviour Analysis Started	OK

2025-08-29 22:16:57	Android Behaviour Analysis Completed	OK
2025-08-29 22:16:57	Extracting Emails and URLs from Source Code	OK
2025-08-29 22:17:00	Email and URL Extraction Completed	OK
2025-08-29 22:17:00	Extracting String data from APK	OK
2025-08-29 22:17:00	Extracting String data from Code	OK
2025-08-29 22:17:00	Extracting String values and entropies from Code	OK
2025-08-29 22:17:02	Performing Malware check on extracted domains	OK
2025-08-29 22:17:09	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.