ANDROID STATIC ANALYSIS REPORT

No icon

Human (4.9.0)

File Name:	health.human.app_130.apk
Package Name:	health.human.app
Scan Date:	Sept. 1, 2025, 1:31 p.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	15	2	2	1

FILE INFORMATION

File Name: health.human.app_130.apk
Size: 30.79MB
MD5: ca6ab9854e0033f880074ccc49617fec
SHA1: 4ddfd94f65c94a162a8d03032c7de2725cafc173
SHA256: 4568c40478edaf056da7d4ab212d7e36cb79f6cf0a9734ffdc892bb2680f3e06

APP INFORMATION

App Name: Human
Package Name: health.human.app
Main Activity: health.human.app.MainActivity
Target SDK: 34
Min SDK: 22
Max SDK:
Android Version Name: 4.9.0

Android Version Code: 130

APP COMPONENTS

Activities: 10
Services: 8
Receivers: 7
Providers: 3
Exported Activities: 2
Exported Services: 1
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
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: 2022-09-02 03:53:04+00:00
Valid To: 2052-09-02 03:53:04+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xef9c3e2175848872cf56129e576e7290732e24ad
Hash Algorithm: sha256
md5: 3713b662506181cf3c7527fe2f6f88b5
sha1: 4a6e633e99806d3138f53948cf0b4ad7edda5db3
sha256: 0fb2c35232b57880bf20a8d9d4cb9b5536cd990ba27bdc8288923584c157846b
sha512: 3d8bf9e9c113d762dbfe9d1cf9aa6f36225c1ed24e9b455b2be0bade60247d3dd4ec9edd5f917e069f6f186d5285ab063cdd00370abb63ab25bc819cfd267804
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 79e5623329ade77512e316ecb1936f530c2026424577d7bbd9b9546e506fd939
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
health.human.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
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.
com.samsung.android.mapsagent.permission.READ_APP_INFO	unknown	Unknown permission	Unknown permission from android reference
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>ca6ab9854e0033f880074ccc49617fec.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
<tr><td>Obfuscator</td><td>Kiwi encrypter</td></tr>
</table>
</td></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.BRAND check
Build.DEVICE check
Build.PRODUCT check
Build.BOARD check
Build.TAGS check
SIM operator check
network operator name check
ro.kernel.qemu check</td></tr>
<tr><td>Obfuscator</td><td>Kiwi encrypter</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</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>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE 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>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
health.human.app.MainActivity	Schemes: https://, Hosts: get.human.health, get-human.onelink.me,
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: **1** | INFO: **1**

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

🔍 MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.1-5.1.1, [minSdk=22]	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	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.
3	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.
4	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
5	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.
6	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.
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: **6** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/amazon/a/a/b/b.java com/amazon/a/a/i/b.java com/amazon/a/a/l/c.java com/appsflyer/internal/AFa1vSDK.java com/appsflyer/internal/AFb1bSDK.java com/appsflyer/internal/AFi1fSDK.java
2	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	capacitor/plugin/appsflyer/sdk/AppsFlyerConstantsKt.java com/capacitorjs/plugins/localnotifications/LocalNotificationManager.java com/capacitorjs/plugins/localnotifications/NotificationStorage.java com/capacitorjs/plugins/localnotifications/TimedNotificationPublisher.java com/getcapacitor/AppUUID.java com/getcapacitor/Bridge.java com/getcapacitor/Plugin.java com/revenuecat/purchases/amazon/AmazonBillingKt.java com/revenuecat/purchases/amazon/AmazonCacheKt.java com/revenuecat/purchases/capacitor/PurchasesPlugin.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

NO	ISSUE	SEVERITY	STANDARDS	FILES
	passwords, keys etc.		OWASP MASVS: MSTG-STORAGE-14	com/revenuecat/purchases/common/diagnostics/DiagnosticsHelper.java com/revenuecat/purchases/common/diagnostics/DiagnosticsTracker.java com/revenuecat/purchases/common/offlineentitlements/ProductEntitlementMapping.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 ee/forgr/capacitor_updater/DownloadService.java io/capawesome/capacitorjs/plugins/firebase/authentication/FirebaseAuthenticationHelper.java
				capacitor/plugin/appsflyer/sdk/AFHelpers.java com/amazon/a/a/g/d.java com/amazon/a/a/o/c.java com/amazon/c/a/a/d.java 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

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/amazon/device/simplesignin/a/c/b.java com/appsflyer/internal/AFg1aSDK.java com/getcapacitor/Logger.java com/getcapacitor/community/inappreview/InAppReview.java com/revenuecat/purchases/capacitor/PurchasesPlugin.java com/revenuecat/purchases/common/DefaultLogHandler.java com/revenuecat/purchases/hybridcommon/CommonKt.java com/revenuecat/purchases/hybridcommon/mappers/PurchasesPeriod.java ee/forgr/capacitor_updater/CapacitorUpdater.java ee/forgr/capacitor_updater/CapacitorUpdaterPlugin.java ee/forgr/capacitor_updater/CryptoCipher.java ee/forgr/capacitor_updater/DownloadService.java io/capawesome/capacitorjs/plugins/firebase/authentication/handlers/AppleAuthProviderHandler.java io/capawesome/capacitorjs/plugins/firebase/authentication/handlers/FacebookAuthProviderHandler.java io/capawesome/capacitorjs/plugins/firebase/authentication/handlers/GoogleAuthProviderHandler.java io/capawesome/capacitorjs/plugins/firebase/authentication/handlers/OAuthProviderHandler.java io/capawesome/capacitorjs/plugins/firebase/authentication/handlers/PlayGamesAuthProviderHandler.java jp/rdlabo/capacitor/plugin/screenshotevent/ScreenshotEvent.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	ee/forgr/capacitor_updater/CryptoCipher.java ee/forgr/capacitor_updater/CryptoCipherV2.java
5	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/capacitorjs/plugins/clipboard/Clipboard.java
6	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
7	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/amazon/a/a/o/b/a.java com/revenuecat/purchases/common/UtilsKt.java
8	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/capacitorjs/plugins/filesystem/Filesystem.java com/getcapacitor/BridgeWebChromeClient.java com/getcapacitor/FileUtils.java jp/rdlabo/capacitor/plugin/screenshotevent/ScreenshotEventPlugin.java
9	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

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/getcapacitor/BridgeWebChromeClient.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/amazon/a/a/i/a.java com/amazon/a/a/i/g.java com/amazon/device/iap/internal/a/a.java com/appsflyer/internal/AFc1bSDK.java com/appsflyer/internal/AFc1kSDK.java com/appsflyer/internal/AFf1tSDK.java com/capacitorjs/plugins/browser/BrowserPlugin.java com/capacitorjs/plugins/localnotifications/LocalNotificationManager.java com/capacitorjs/plugins/localnotifications/LocalNotificationsPlugin.java com/capacitorjs/plugins/share/SharePlugin.java com/getcapacitor/Bridge.java io/capawesome/capacitorjs/plugins/firebase/authentication/FirebaseAuthentication.java nl/raphael/settings/NativeSettingsPlugin.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/amazon/a/a/i/g.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFj1tSDK.java com/appsflyer/internal/AFj1wSDK.java com/appsflyer/internal/AFj1xSDK.java com/capacitorjs/plugins/browser/Browser.java com/capacitorjs/plugins/localnotifications/LocalNotificationManager.java com/capacitorjs/plugins/localnotifications/NotificationChannelManager.java com/capacitorjs/plugins/pushnotifications/NotificationChannelManager.java com/capacitorjs/plugins/share/SharePlugin.java com/getcapacitor/AndroidProtocolHandler.java com/getcapacitor/Bridge.java com/getcapacitor/plugin/util/AssetUtil.java
00096	Connect to a URL and set request method	command network	com/appsflyer/internal/AFd1hSDK.java com/appsflyer/internal/AFe1lSDK.java com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/HttpRequestHandler.java com/revenuecat/purchases/common/HTTPClient.java ee/forgr/capacitor_updater/DownloadService.java
00089	Connect to a URL and receive input stream from the server	command network	com/appsflyer/internal/AFd1hSDK.java com/appsflyer/internal/AFe1lSDK.java com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java com/revenuecat/purchases/common/HTTPClient.java ee/forgr/capacitor_updater/DownloadService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/appsflyer/internal/AFd1hSDK.java com/appsflyer/internal/AFe1lSDK.java com/appsflyer/internal/AFf1kSDK.java com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/HttpRequestHandler.java com/revenuecat/purchases/common/HTTPClient.java ee/forgr/capacitor_updater/DownloadService.java
00015	Put buffer stream (data) to JSON object	file	ee/forgr/capacitor_updater/CapacitorUpdater.java
00014	Read file into a stream and put it into a JSON object	file	com/appsflyer/internal/AFg1jSDK.java ee/forgr/capacitor_updater/CapacitorUpdater.java
00022	Open a file from given absolute path of the file	file	com/amazon/a/a/b/b.java com/appsflyer/internal/AFg1jSDK.java com/capacitorjs/plugins/filesystem/Filesystem.java com/capacitorjs/plugins/filesystem/FilesystemPlugin.java com/getcapacitor/FileUtils.java com/getcapacitor/plugin/util/AssetUtil.java ee/forgr/capacitor_updater/CapacitorUpdater.java ee/forgr/capacitor_updater/DownloadService.java
00013	Read file and put it into a stream	file	com/amazon/c/a/a/c.java com/appsflyer/internal/AFa1ySDK.java com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFg1jSDK.java com/capacitorjs/plugins/filesystem/Filesystem.java com/getcapacitor/AndroidProtocolHandler.java com/revenuecat/purchases/common/FileHelper.java ee/forgr/capacitor_updater/CapacitorUpdater.java ee/forgr/capacitor_updater/DownloadService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/AFg1jSDK.java ee/forgr/capacitor_updater/CapacitorUpdater.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 com/appsflyer/internal/AFb1rSDK.java com/appsflyer/internal/AFc1kSDK.java com/capacitorjs/plugins/pushnotifications/PushNotificationsPlugin.java com/getcapacitor/Bridge.java ee/forgr/capacitor_updater/CapacitorUpdater.java
00121	Create a directory	file command	ee/forgr/capacitor_updater/CapacitorUpdater.java
00024	Write file after Base64 decoding	reflection file	com/capacitorjs/plugins/filesystem/Filesystem.java ee/forgr/capacitor_updater/CapacitorUpdater.java
00004	Get filename and put it to JSON object	file collection	ee/forgr/capacitor_updater/CapacitorUpdater.java
00012	Read data and put it into a buffer stream	file	com/amazon/c/a/a/c.java ee/forgr/capacitor_updater/CapacitorUpdater.java
00125	Check if the given file path exist	file	com/getcapacitor/Bridge.java ee/forgr/capacitor_updater/CapacitorUpdater.java
00104	Check if the given path is directory	file	ee/forgr/capacitor_updater/CapacitorUpdater.java

RULE ID	BEHAVIOUR	LABEL	FILES
00094	Connect to a URL and read data from it	command network	com/capacitorjs/plugins/filesystem/Filesystem.java com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java ee/forgr/capacitor_updater/CapacitorUpdater.java ee/forgr/capacitor_updater/DownloadService.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/AFi1rSDK.java
00072	Write HTTP input stream into a file	command network file	com/getcapacitor/plugin/util/AssetUtil.java ee/forgr/capacitor_updater/DownloadService.java
00108	Read the input stream from given URL	network command	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java ee/forgr/capacitor_updater/DownloadService.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	nl/raphael/settings/NativeSettingsPlugin.java
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFj1tSDK.java com/appsflyer/internal/AFj1uSDK.java com/appsflyer/internal/AFj1vSDK.java com/appsflyer/internal/AFj1xSDK.java com/getcapacitor/FileUtils.java
00030	Connect to the remote server through the given URL	network	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java
00123	Save the response to JSON after connecting to the remote server	network command	com/getcapacitor/plugin/util/CapacitorHttpUrlConnection.java com/getcapacitor/plugin/util/HttpRequestHandler.java

RULE ID	BEHAVIOUR	LABEL	FILES
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1lSDK.java com/getcapacitor/FileUtils.java
00028	Read file from assets directory	file	com/getcapacitor/FileUtils.java
00153	Send binary data over HTTP	http	com/getcapacitor/plugin/util/CapacitorHttpUrlConnection.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1lSDK.java com/appsflyer/internal/AFj1uSDK.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFb1lSDK.java com/appsflyer/internal/AFj1uSDK.java
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFj1uSDK.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFj1uSDK.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFj1uSDK.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFj1uSDK.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/1015641237586/namespaces/firebase:fetch?key=AIzaSyCcUFBOeZAWGDlIZ7kURmU1oIWx3xJzPmg. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.INTERNET, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	3/44	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
www.risktabsprev10pxrise25pxblueding300ballfordearnwildbox.fairlackverspairjunetechifpickevil	ok	No Geolocation information available.
www.wencodeuricomponent	ok	No Geolocation information available.
www.css	ok	No Geolocation information available.
www.interpretation	ok	No Geolocation information available.
sinapps.s	ok	No Geolocation information available.
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.world	ok	**IP:** 99.83.155.228 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
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
www.years	ok	No Geolocation information available.
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
.css	ok	No Geolocation information available.
sconversions.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
capacitorjs.com	ok	**IP:** 104.21.93.31 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sattr.s	ok	No Geolocation information available.
www.a	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
www.hortcut	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
sars.s	ok	No Geolocation information available.
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
www.manifestations	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
scdn-ssettings.s	ok	No Geolocation information available.
www.googleorganizationautocompleterequirementsconservative	ok	No Geolocation information available.
www.in	ok	No Geolocation information available.
www.language	ok	No Geolocation information available.
scdn-stestsettings.s	ok	No Geolocation information available.
api-diagnostics.revenuecat.com	ok	**IP:** 54.88.247.37 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.recent	ok	No Geolocation information available.
aps-webhandler.appsflyer.com	ok	**IP:** 18.238.109.114 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api-paywalls.revenuecat.com	ok	**IP:** 54.243.244.245 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
sonelink.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
svalidate-and-log.s	ok	No Geolocation information available.
api.capgo.app	ok	**IP:** 172.66.43.166 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sapp.s	ok	No Geolocation information available.
www.icon	ok	No Geolocation information available.
www.c	ok	No Geolocation information available.

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:** 18.238.109.111 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sviap.s	ok	No Geolocation information available.
www.style	ok	**IP:** 99.83.155.228 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
.jpg	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
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
svalidate.s	ok	No Geolocation information available.
api.revenuecat.com	ok	**IP:** 13.223.22.191 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.text-decoration	ok	No Geolocation information available.

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
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"google_api_key" : "AIzaSyCcUFBOeZAWGDlIZ7kURmU1oIWx3xJzPmg"
"google_crash_reporting_api_key" : "AIzaSyCcUFBOeZAWGDlIZ7kURmU1oIWx3xJzPmg"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166438125740282911150571 51
470fa2b4ae81cd56ecbcda9735803434cec591fa
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
af60eb711bd85bc1e4d3e0a462e074eea428a8
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMlM=

POSSIBLE SECRETS
36864200e0eaf5284d884a0e77d31646
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
115792089210356248762697446949407573530086143415290314195533631308867097853951
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
bae8e37fc83441b16034566b
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: Human Health Tracker

Score: 4.16 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** health.human.app

Developer Details: Human Operations Pty Ltd, Human+Operations+Pty+Ltd, None, https://human.health, support@human.health,

Release Date: Apr 20, 2023 **Privacy Policy:** Privacy link

Description:

□ Human Health: Symptom Tracker, Medication Reminder & Digital Health Record The ultimate app to track symptoms, medications & treatments, turning your daily experience into actionable data. With Human Health, you can create a secure digital health record to monitor how your symptoms or overall health are changing over time. Designed with input from patients, parents & medical experts from top US hospitals & universities, Human Health helps manage symptoms & treatments for chronic conditions, mental health, neurological disorders, pain, autoimmune diseases & more. Key Features: □ SYMPTOM TRACKER & HEALTH JOURNAL - Track over 1700+ symptoms daily, including chronic symptoms, mental health symptoms, neurological symptoms, pain symptoms, autoimmune symptoms, and gastrointestinal symptoms. - Get personalized insights into how symptoms change over time. - Add photos and notes to symptoms for more in-depth information. - Create a mood journal to monitor mental health symptoms like stress, anxiety, depression, and emotional well-being. □ MEDICATION REMINDER, TREATMENTS LOG & PILL TRACKER - Log medications, treatments, and supplements with custom reminders. - Track 100,000+ treatments, including therapies, assistive devices, and lifestyle changes. - Create a flexible medication & treatment plan: choose medication frequency that works for you. - Track medication & treatment adherence & compare it to your symptom data □ MENTAL HEALTH TRACKER & MOOD JOURNAL - Log mental health symptoms like anxiety, depression, & mood swings. - Track mental health patterns & understand mood fluctuations. - See how medications & lifestyle changes impact mental health. - Journal to better manage your mental health. □⚕ DOCTOR READY HEALTH REPORTS - Generate a free 3-month health summary (symptom & medications) for doctor visits. - Customizable reports for greater flexibility to highlight relevant symptoms & medication changes e.g. only include mental health symptoms and mental health medications for therapists. - Store & access lab results, scans, & medical records for easy access. □ FAMILY SYMPTOM & MEDICATION TRACKING - Create multiple profiles for your family in Human Health. - Use Human Health as your own symptom tracker & medication reminder - Use Human Health as a symptom tracker & medication reminder for your family. □ YOUR PRIVACY, OUR PRIORITY -Encrypted and protected data, with control over who views your information. -Your personal data will never be sold, and you can delete it anytime. -Always accessible data—download, export, or delete files when needed. For more information, visit: https://humanhealth.zendesk.com/hc/en-us Privacy Policy: https://humanhealth.zendesk.com/hc/en-us/articles/17643897206681-Our-Privacy-Policy For support, email: support@human.health Insights provided by Human Health do not constitute medical advice. Always consult your doctor before making any medical decisions.

SCAN LOGS

Timestamp	Event	Error

2025-09-01 13:31:47	Generating Hashes	OK
2025-09-01 13:31:47	Extracting APK	OK
2025-09-01 13:31:47	Unzipping	OK
2025-09-01 13:31:47	Parsing APK with androguard	OK
2025-09-01 13:31:47	Extracting APK features using aapt/aapt2	OK
2025-09-01 13:31:47	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 13:31:49	Parsing AndroidManifest.xml	OK
2025-09-01 13:31:49	Extracting Manifest Data	OK
2025-09-01 13:31:49	Manifest Analysis Started	OK
2025-09-01 13:31:50	Performing Static Analysis on: Human (health.human.app)	OK
2025-09-01 13:31:52	Fetching Details from Play Store: health.human.app	OK

2025-09-01 13:31:53	Checking for Malware Permissions	OK
2025-09-01 13:31:53	Fetching icon path	OK
2025-09-01 13:31:54	Library Binary Analysis Started	OK
2025-09-01 13:31:54	Reading Code Signing Certificate	OK
2025-09-01 13:31:54	Running APKiD 2.1.5	OK
2025-09-01 13:31:59	Detecting Trackers	OK
2025-09-01 13:32:01	Decompiling APK to Java with JADX	OK
2025-09-01 13:32:15	Converting DEX to Smali	OK
2025-09-01 13:32:15	Code Analysis Started on - java_source	OK
2025-09-01 13:32:16	Android SBOM Analysis Completed	OK
2025-09-01 13:32:20	Android SAST Completed	OK

2025-09-01 13:32:20	Android API Analysis Started	OK
2025-09-01 13:32:23	Android API Analysis Completed	OK
2025-09-01 13:32:23	Android Permission Mapping Started	OK
2025-09-01 13:32:26	Android Permission Mapping Completed	OK
2025-09-01 13:32:26	Android Behaviour Analysis Started	OK
2025-09-01 13:32:29	Android Behaviour Analysis Completed	OK
2025-09-01 13:32:29	Extracting Emails and URLs from Source Code	OK
2025-09-01 13:32:30	Email and URL Extraction Completed	OK
2025-09-01 13:32:30	Extracting String data from APK	OK
2025-09-01 13:32:30	Extracting String data from Code	OK
2025-09-01 13:32:30	Extracting String values and entropies from Code	OK

2025-09-01 13:32:33	Performing Malware check on extracted domains	OK
2025-09-01 13:32:36	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.

© 2025 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.