MOBSF

ANDROID STATIC ANALYSIS REPORT

PineApp (6.0)

File Name:	com.osellus.android.pineapp_1004146.apk
Package Name:	com.osellus.android.pineapp
Scan Date:	Sept. 1, 2025, 6:48 a.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	23	2	2	2

FILE INFORMATION

File Name: com.osellus.android.pineapp_1004146.apk
Size: 23.19MB
MD5: 0f752b1e3e3129b1544e176aa8be3dbd
SHA1: 3520605ddca2e78f23372dc5a3b35582c59ad144
SHA256: 67e539542456b1a63fab82c0f199a1c15f48eb77c2227807d6a9cbfaeb74a546

APP INFORMATION

App Name: PineApp
Package Name: com.osellus.android.pineapp
Main Activity: com.batisthealth.pine.MainActivity
Target SDK: 35
Min SDK: 26
Max SDK:
Android Version Name: 6.0

Android Version Code: 1004146

APP COMPONENTS

Activities: 10
Services: 22
Receivers: 15
Providers: 6
Exported Activities: 1
Exported Services: 2
Exported Receivers: 9
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: OU=osellus inc., CN=james
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2011-01-19 21:56:01+00:00
Valid To: 2036-01-13 21:56:01+00:00
Issuer: OU=osellus inc., CN=james
Serial Number: 0x4d375df1
Hash Algorithm: sha1
md5: 94cefd680bf526e5216f49d9b01a0b34
sha1: 59172d18f3dd5bff61fba44a5f819322e4753322
sha256: 2d0ef0e3d8fc967842de319072196707d850900e0d6e185835c13b02c9321080
sha512: c2db4cbd9aa54ae2b250c0864e1e7c05ca5e944e5b6e7feacb9f9c38e0d4ad469456c8a998c9409f385acd5ea1c4f3f4c895f50a12b8c6207be2409df9d7c78c
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 9ee4190366dde970b663354a091589d8c85ee35dddd5e5b18b5f648d32c21ae1
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.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.pineapp.prod.permission.DEEPLINK	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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.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.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
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.BROADCAST_CLOSE_SYSTEM_DIALOGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.BIND_NOTIFICATION_LISTENER_SERVICE	signature	required by NotificationListenerServices for system binding.	Must be required by an NotificationListenerService, to ensure that only the system can bind to it.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
Manifest.permission.CAPTURE_AUDIO_OUTPUT	unknown	Unknown permission	Unknown permission from android reference
com.osellus.android.pineapp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
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.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.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.

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

APKID ANALYSIS

FILE	DETAILS
0f752b1e3e3129b1544e176aa8be3dbd.apk	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>possible VM check</td></tr></table>

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 subscriber ID 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>

<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
Build.TAGS check
network operator name check
possible ro.secure 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>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.batisthealth.pine.MainActivity	Schemes: https://, bhsf://, Hosts: pineapp.web.baptisthealth.net, pineapp, deeplink.pine.app, pineappbaptisthealth.page.link,
com.google.android.gms.tagmanager.TagManagerPreviewActivity	Schemes: tagmanager.c.com.batisthealth.pine.stg://, tagmanager.c.com.osellus.android.pineapp://,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 0 | WARNING: 13 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Activity (com.google.android.gms.tagmanager.TagManagerPreviewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Broadcast Receiver (me.carda.awesome_notifications.DartNotificationActionReceiver) 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 (me.carda.awesome_notifications.DartDismissedNotificationReceiver) 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.
5	Broadcast Receiver (me.carda.awesome_notifications.DartScheduledNotificationReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Broadcast Receiver (me.carda.awesome_notifications.DartRefreshSchedulesReceiver) 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.pravera.flutter_activity_recognition.service.ActivityRecognitionIntentReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
9	Broadcast Receiver (com.pravera.flutter_foreground_task.service.RebootReceiver) 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.
10	Service (me.carda.awesome_notifications.core.managers.StatusBarManager) 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.
11	Service (androidx.health.platform.client.impl.sdkservice.HealthDataSdkService) 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.
12	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.
13	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: 8 | INFO: 2 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A/T.java A8/a.java B0/A.java B0/AbstractC0563b.java B0/AbstractC0566c0.java B0/C0605w0.java B0/U.java B3/q.java B4/k.java B9/AbstractC0658l.java B9/C0634f.java B9/C0653j2.java B9/C0685s.java C0/t.java C8/B.java C8/D.java C8/i.java E1/c.java E3/a.java E3/e.java E4/a.java E9/a.java F1/a.java G0/c.java G8/d.java H0/j.java H3/f.java H3/o.java Ia/b.java Ia/d.java Ia/e.java Ia/i.java Ia/m.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				Ia/m.java K5/w.java L0/c.java M/y.java M1/d.java M1/e.java M1/f.java M3/a.java M5/g.java M6/a.java M6/b.java M6/c.java M7/m.java O/d.java O1/a.java O3/e.java S3/L0.java S7/o.java S7/q.java S8/b.java T1/a.java W1/a.java W5/c.java X0/a.java X0/b.java X7/a.java X7/b.java X7/c.java Y3/j.java Y7/a.java Y7/e.java Z3/b.java Z7/h.java a0/C1308b.java a1/C1318c.java b2/AbstractC1404o.java b4/C1422a.java b4/p.java b4/r.java b4/v.java b8/AbstractC1442a.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	b87b.java c0/C1454d.java c8/AbstractC1507e.java c8/C1505c.java com/baseflow/geolocator/GeolocatorLocationService.java com/baseflow/geolocator/b.java com/baseflow/geolocator/j.java com/baseflow/geolocator/m.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 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/InAppWebViewChr

NO	ISSUE	SEVERITY	STANDARDS	FILES
				omeClient.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 e/AbstractC1563e.java f0/f.java io/flutter/plugins/firebase/crashlytics/a.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 l/C2087d.java l/C2088e.java l/C2089f.java l/h.java l/i.java l/k.java l/l.java l9/C2173f2.java l9/W1.java m0/d.java m0/e.java m0/m.java m0/r.java m0/y.java m6/C2655d.java me/carda/awesome_notifications/core/databases/SqLiteCypher.java me/carda/awesome_notifications/core/logs/Logger.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				n/AbstractC2671c.java p0/AbstractC2673a.java n6/AbstractC2688b.java p0/AbstractC2734c.java p0/AbstractC2739h.java p0/C2735d.java p3/n.java p6/g.java p8/e.java q0/AbstractC2816e.java q0/AbstractC2818g.java q0/C2819h.java q0/l.java q4/C2870b.java q9/AbstractC2876a.java r4/AbstractC2952a.java s2/l.java t9/p.java v6/e.java v9/i.java w3/c.java w4/AbstractC3205a.java w9/k.java wa/c.java x0/g.java x0/l.java x3/AbstractC3248a.java x9/C3273C.java x9/C3276a.java y/W.java y0/d.java y3/AbstractC3349E.java y3/C3364e.java y9/C3417i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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 OWASP MASVS: MSTG-STORAGE-14	c2/C1462a.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 l5/C2104a.java me/carda/awesome_notifications/core/Definitions.java me/carda/awesome_notifications/core/databases/SQLitePrimitivesDB.java me/carda/awesome_notifications/core/databases/SQLiteSchedulesDB.java n/AbstractC2670b.java x9/C3272B.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	C8/i.java I4/M.java I4/W.java com/pichillilorenzo/flutter_inappwebview_android/credential_database/CredentialDatabaseHelper.java me/carda/awesome_notifications/core/databases/SQLitePrimitivesDB.java me/carda/awesome_notifications/core/databases/SQLiteSchedulesDB.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	N4/q0.java S3/AbstractC1128h0.java S3/C1160y.java T3/a.java ca/AbstractC1509a.java ca/C1510b.java da/C1558a.java g2/C1727r0.java i2/C1827b.java p5/S.java s5/b.java v2/d0.java y8/d.java
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	X7/a.java X7/b.java X7/c.java c8/AbstractC1507e.java f4/e.java n0/AbstractC2674b.java v9/h.java v9/i.java
6	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	A/C0506u.java X0/a.java c8/AbstractC1507e.java l9/K2.java l9/R1.java
7	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	z8/AbstractC3489a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	me/carda/awesome_notifications/core/utils/StringUtils.java
9	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	r2/AbstractC2947b.java
10	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	Z7/h.java l/i.java u5/C3079a.java
11	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 j9/C1977g.java
12	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	v6/s.java z8/C3490b.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00028	Read file from assets directory	file	J5/C0854c.java d2/C1515a.java
00096	Connect to a URL and set request method	command network	J5/u.java com/pichillilorenzo/flutter_inappwebview_android/Util.java d2/C1526l.java
00089	Connect to a URL and receive input stream from the server	command network	J5/u.java d2/C1526l.java
00030	Connect to the remote server through the given URL	network	J5/u.java com/pichillilorenzo/flutter_inappwebview_android/Util.java d2/C1526l.java
00109	Connect to a URL and get the response code	network command	J5/u.java d2/C1526l.java
00094	Connect to a URL and read data from it	command network	J5/u.java com/pichillilorenzo/flutter_inappwebview_android/Util.java d2/C1526l.java
00108	Read the input stream from given URL	network command	J5/u.java d2/C1526l.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	G8/d.java O3/e.java V3/a.java a4/AbstractC1329a.java b4/C1422a.java b4/p.java b4/v.java c8/C1505c.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 d4/C1541a.java e4/C1582a.java me/carda/awesome_notifications/core/managers/PermissionManager.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java n/AbstractC2671c.java p9/C2792h.java t9/l.java v8/AbstractC3188c.java y9/C3416h.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	O3/e.java a4/AbstractC1329a.java b4/C1422a.java b4/p.java b4/v.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserManager.java e4/C1582a.java me/carda/awesome_notifications/core/managers/PermissionManager.java v8/AbstractC3188c.java y9/C3416h.java
00036	Get resource file from res/raw directory	reflection	G8/d.java J5/J.java O3/e.java a4/AbstractC1329a.java b4/C1422a.java b4/p.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java d2/C1536v.java me/carda/awesome_notifications/core/managers/ChannelManager.java me/carda/awesome_notifications/core/managers/PermissionManager.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java v8/AbstractC3188c.java
00161	Perform accessibility service action on accessibility node info	accessibility service	C0/t.java io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/c.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	C0/t.java io/flutter/view/AccessibilityViewEmbedder.java

RULE ID	BEHAVIOUR	LABEL	FILES
00189	Get the content of a SMS message	sms	X7/c.java
00192	Get messages in the SMS inbox	sms	X7/c.java
00188	Get the address of a SMS message	sms	X7/c.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	X7/c.java g4/C1746b.java
00191	Get messages in the SMS inbox	sms	X7/c.java
00200	Query data from the contact list	collection contact	X7/c.java
00201	Query data from the call log	collection calllog	X7/c.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	X7/c.java
00023	Start another application from current application	reflection control	V3/a.java e4/C1582a.java
00003	Put the compressed bitmap data into JSON object	camera	com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebView.java
00038	Query the phone number	collection	S3/x1.java
00066	Query the ICCID number	collection	S3/x1.java
00067	Query the IMSI number	collection	S3/x1.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	A/C0506u.java F9/b.java N0/m.java Q/Q.java S3/C1137m.java X0/a.java X7/b.java X8/f.java c8/AbstractC1507e.java f4/e.java l9/R1.java me/carda/awesome_notifications/core/utils/BitmapUtils.java q4/C2869a.java q4/C2870b.java v4/C3171a.java v9/i.java
00013	Read file and put it into a stream	file	A/C0506u.java C3/G.java J5/C0860i.java J5/J.java N0/m.java S3/C1124f0.java S3/P0.java U9/i.java U9/k.java X0/a.java c8/AbstractC1507e.java com/pichillilorenzo/flutter_inappwebview_android/Util.java d2/C1518d.java d2/C1536v.java m0/e.java q0/l.java q4/C2870b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	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 me/carda/awesome_notifications/core/builders/NotificationBuilder.java
00199	Stop recording and release recording resources	record	Ia/o.java
00198	Initialize the recorder and start recording	record	Ia/o.java
00194	Set the audio source (MIC) and recorded file format	record	Ia/o.java
00197	Set the audio encoder and initialize the recorder	record	Ia/o.java
00196	Set the recorded file format and output path	record file	Ia/o.java
00012	Read data and put it into a buffer stream	file	X0/a.java c8/AbstractC1507e.java
00132	Query The ISO country code	telephony collection	K5/T.java b2/AbstractC1388K.java
00209	Get pixels from the latest rendered image	collection	T8/l.java

RULE ID	BEHAVIOUR	LABEL	FILES
00210	Copy pixels from the latest rendered image into a Bitmap	collection	T8/l.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	a2/C1326a.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebViewChromeClient.java u4/C3078a.java
00202	Make a phone call	control	b4/v.java
00203	Put a phone number into an intent	control	b4/v.java
00045	Query the name of currently running application	collection reflection	S3/E.java
00175	Get notification manager and cancel notifications	notification	m0/r.java
00035	Query the list of the installed packages	reflection	S3/P0.java
00123	Save the response to JSON after connecting to the remote server	network command	com/pichillilorenzo/flutter_inappwebview_android/Util.java
00102	Set the phone speaker on	command	x8/C3262E.java
00056	Modify voice volume	control	x8/C3262E.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/423493082241/namespaces/firebase:fetch?key=AIzaSyAcYO52W7HiQwSkcndhmrRtCEG9oKsPFAk. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.WAKE_LOCK, android.permission.CAMERA, android.permission.VIBRATE, android.permission.READ_PHONE_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.RECORD_AUDIO, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	12/44	android.permission.ACCESS_BACKGROUND_LOCATION, com.google.android.gms.permission.ACTIVITY_RECOGNITION, android.permission.ACTIVITY_RECOGNITION, android.permission.READ_CALENDAR, android.permission.ACCESS_NOTIFICATION_POLICY, android.permission.FOREGROUND_SERVICE, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, 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
ns.adobe.com	ok	No Geolocation information available.
aomedia.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **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

DOMAIN	STATUS	GEOLOCATION
g.co	ok	**IP:** 172.217.21.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
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
pineapp.web.baptisthealth.net	ok	**IP:** 18.238.96.8 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
dashif.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
issuetracker.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pub.dev	ok	**IP:** 34.36.0.14 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
developer.apple.com	ok	**IP:** 17.253.83.133 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
default.url	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
www.example.com	ok	**IP:** 23.220.73.43 **Country:** Colombia **Region:** Antioquia **City:** Medellin **Latitude:** 6.251840 **Longitude:** -75.563591 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "5d04d732e8354d07bf6b8626ceb0a2ab"
"google_api_key" : "AIzaSyAcYO52W7HiQwSkcndhmrRtCEG9oKsPFAk"
"google_crash_reporting_api_key" : "AIzaSyAcYO52W7HiQwSkcndhmrRtCEG9oKsPFAk"
03770B6AF9204D14D0435B03613F1F65FB5613172B43613151BB797E3B95B9370F7C0B31F1711F18D0425F04336B4F36A7521E4A2C44613D01ED232C6E95B53B
5425014DB1264C5490117E5B3C601D3CFB3759467217056059BA73
76311B60AC2D5B4887357070

POSSIBLE SECRETS
5B21016FBD2B0F5185065C5971600921EB42484A3C17206D51AD7E682882E46E59645F
55310664AD104A4D8D1A484C017F1322FA105E56
64301D61A7246D548D1859512325557CFE125A436558307D59B57F7F7AB7EF7B5E2B0121E73740729006545A362555
542B0226AD26594887114F5B3E795239F60C4D5C7D1C3E6C55AF72796DD8E86A412D0C6DBB2C40558F1D5353
542B0226BD2B465380045C4625745221EA124F5D6903377A
56281B6DBB2D4E558D025877347F081AFE11424A6F
723C1F6DAA37464F83545F5D3F691920BF005F5B3C173D7C10B76E7664D7AC2F
542C0A6BA20D4E558D0258793479143DFB11
542B0226A1364E56811D135C266418
542C0A6BA210464CB7114F5D3061
9a04f079-9840-4286-ab92-e65be0885f95
5826097DBA204E558D1B537D227E0937EC
1837167BBD26420E9716545A
5321417AA621590F851A59463E64187CE712455C79147C615EAA6F7B649AE97D
55310664AD265D0F901B6E4023641235B74B

POSSIBLE SECRETS
47251C7BAA2C4B44BB075840
e2719d58-a985-b3c9-781a-b030af78d30e
5E2A067CE7305942CA025F5B29354A7FEC075E5A6C
47211D6EA6314263881B5E5F71767672BF420A0F3C507228D259BD3221DAAC7B45310A24E9375D54815D3714712D5C72BF420A52
542B0226A22A4146961B52407F66153CF817594A6E
5E2A067CE7305942CA10585921680A37F11646407B
723C1F6DAA374A45B4155E5F306A191CFE0F4F0F7503726645B57734
5F251C5AA62C5B488A136D5532661D35FA1163416F0433645CBC7F
VGhpcyBpcyB0aGUga2V5IGZvcihBIHNlY3XyZZBzdG9yYWdlIEFFUyBLZXkK
6325037BAC2070649C0058463F6C10
013515318E316715D5187557235B1D18C63A4D7574390360529F296B4FB5BE407F22
15200A7EA0204A688056074F5B2D5C72BF420A0D7D1E367A5FB07F536CD4B62D
50211B50B92C5C44802258462264133C
1837167BBD26420E85044D1B
4E3D1671E40E620C80101A6076453468F20F105C6F5E015B638A484952

POSSIBLE SECRETS
6325037BAC200F628B1A5B5D362D1F33F10C455B3C1237285EAC777626
15686528E9630F01C456505135641D16ED0F08153E
622A0E6AA5260F558B545A51252D1A3BF1054F5D6C023B6644BC693A6198FF7B562A0C6DE7
1837167BBD26420E861D53
5A21417FAC2A5C49915A584C21
72361D67BB63404287014F4634695C25F70B464A3C02377C42B07E6C6198EB2F5C211628A02D494EC4124F5B3C2D1737E6115E406E15
70770C72FA216A47A11F7A0417553E34D9376F1A5E3221506295522D6387FA6D6502
5B2B086FA02D487297186D5D3F63153CF8
1837167BBD26420E9C16545A7E6009
542B0226BA225A538D1F1347246F0F26ED035E4A
5E2A067CE7305942CA195C53387E170DEF04594B
422A006EAF2A4C488518745A22791D3EF3035E46731E016745AB787F4697F8664121
7021017DA02D4A688A005858
72361D67BB63404287014F4634695C25F70B464A3C06336459BD7A6E6198EB2F53251B69E925405389545651287E083DED07
562A0B7AA62A4B0F94114F59387E0F3BF00C04695322174F62964E544CA9DF4A6512264B8C

POSSIBLE SECRETS
51210E7CBC314A758107495D3F6A3535F10D584A78
422A006EAF2A4C488518745A22791D3EF3035E46731E016745AB787F
542C0A6BA20642548815495B235D0E3DEF07585B6526336445BC68
72361D67BB6358498D185814306E1F37EC1143417B50107D59B57F344AB9CD5D73640961AC2F4B
562A0B7AA62A4B0F94114F59387E0F3BF00C047F532306577E964F534EBFCF4E630D20469A
532D086DBA3701458D135847252555
5425014DB1264C5490117E5B3C601D3CFB
542B0226BA2A4B40CA1A58433A641235ED0D455B751E217C51B5777F7A93ED7C4E
04755F3AFF731F11D4440D04613D4C
542B0226A82F4A518C0E5C5D3F231A20FE0F4B5D731F26
56360A49B9285C6092155458306F1037
712A297A8E2C7F40D63F0B7A3D5D2C2AC50A4D64283C275264BD57707E94F87A0E2E0871A12C1944
542B0226AD2A424E8A0254503462523EEA0141566C11266B58BC69
76013C278A016C0EAA1B6D553569153CF8
5F301B78BA79000ED0175850633F1F33AF541C4B2813333C51EE2C283E95B56E51220930AA731C18CA014E19346C0F26B253044E6B037C6E5FAC757E269FE3350E765B3BE6374E4D97115E6B3D621B0DEF10454B43113C6C42B6727E5790FE6A521B187AA0374A0EBB1052576E7D1522FA0E4341794D26695CAA7E79579AE368682D016CAC3B

POSSIBLE SECRETS
031E264A903A664EBC225B0509753813D12B7E474F4417625DE1574F729FFE5B46
562A0B7AA62A4B0F94114F59387E0F3BF00C04665224175A7E9C4F
44210361A736576C8B1058
5E371C7DAC316E4D90114F5A30791524FA2C4B427903
762A0B7AA62A4B01B73076143378153EEB424C406E502A3006
5E2A067CE7305942CA1254583460133C
40130E4C86027B16D2265E6C183D143BDD2E707845401C4B01B32B7F4C98FC3D6F2B2E648E095E53
562A0B7AA62A4B0F94114F59387E0F3BF00C0467553417577F8F5E4844B7D550600D214C86147C
72361D67BB6358498D185814306E1F37EC1143417B50107D59B57F3445B9C84A7B640961AC2F4B
622A0E6AA5260F558B544F51257F1537E9070A4C7902266156B0787B7C93AC675E371B67BB3A01
44210C7DBB2A5B58B415495739
542B0226A22C5A528C1D565024790833B1115F5F7902277B55AB
5F2B0063AC270F54971D535371550C3DEC074E
47250C63A8244A6C851A5C53347F5235FA1663416F043364D259BD7B6F93C16E5925086DBB6D6864B02B7071054C2316DE366B06

POSSIBLE SECRETS
542C0A6BA20642548815495B234F0E33F106
58360826A42640568715491A34690422F0114F4B321D336651BE7E68
47250C63A8244A6F851958
542B0278A62D4A4F903C585523791E37FE16
59282D3FFC1A1C19D1375B7B15444E25FC37607F451F1E4E07955C296AB2EE437B2B00
5E373D7DA72D464F8327486423621F37EC114F5C5D13266146B06F634597E26E50211D
53211961AA267C55850058
74731E4B852469588D3751043E7C116BA7376B5E45
5F332D69AA284A45AF114457396C153C
56341F41A7374A46961D494D12651931F427585D7302
5231416BA122464F821D4F517F7E0922FA10595A
562A0B7AA62A4B0F94114F59387E0F3BF00C047A4F350D4A7996565F5CA4C54C
67251C7BAC270F548A07484421620E26FA060A447909217C5FAB7E
47211D7BA0305B0F89155A5D2266523AF6064F

POSSIBLE SECRETS
5A25017DAF224C5591065846
44210361A7365771961B4D5123791537EC
5E2A0C61AD264155B6114D5B2379
622A0E6AA5260F558B545E5B3C7D0926FA4279675D5D603D06F97F736F93FF7B1722007AE9244657811A1D583E6A52
5232375C87015A178E237F513A7C1F01FE506C425318176D7AA9595B6C91F5694728193F84700079B2034E09
56360A4AA02D4E538D114E6423680F37F116
72361D67BB63404287014F4634695C25F70B464A3C03266742B0757D2892ED7B56641B67E9284A589700524634
5F251C41A7354E4D8D106E5D36631D26EA104F6B7517377B44977A6E6180E9
7E2A1B6DBB2D4E4DC41D4E4724685C3BF1425E477950396D49AA6F757A93AC6D5E2A0B6DBB634B4490115E40346952
56270C6DBA3046438D185440284C0C22EC
542B0226BE394A44961B52400E394E65A653191E32112263
5A25037FA8314A69850755763D6C1F39F30B595B
5E373778A6304A45B2114F4738621213E90343437D123E6D
452B4160A8314B56850658
7A05235F88116A7EAD3A7B7B

POSSIBLE SECRETS
742B017CAC3B5B018715535A3E795C30FA42445A701C7C
446A016DB13763488A11151D
1837167BBD26420E9C16545A7E
76641D6DBA2C5A5387111D5230641037FB425E403C1333645CF9537B7A92FB6E45212D7DAF254A53CA17515B22685272BF
452B4160A8314B568506581A27640E26EA0346707815246153BC
542B0226A1265740891B5F1A39620B26F010454068
422D2B67F1144458963F4C60684B4967DB1B4F174F136B7C459842707E8EC438432A1D38
40251B6BA1265D6C851D51
542B0226AE2C40468811137A3E791534F6014B5B751F3C5B55AB6D736B93
5E37207CA8004A53901D5B5D326C0837D20B595C751E35
622A0466A634410196115C572564133CBF16535F795E
5428007BAC105B53811550
523C0A6BBC37464E8A2749552568
5F251C41A7354E4D8D106E5D36631D26EA104F6B7517377B44
1837167BBD26420E81005E1B38631526B10605162523277855AB484F4C97E962582A

POSSIBLE SECRETS
54211D7CA02546428500587D3F6B13
542B0226AA2B4A4D94014E1A3D781F39E6124B5B7F18377A
042E2950A4247F138C1D496C0267282BD631497D6E25214907BA50225AA5CF595C7659
742C0A6BA20D4E4C814E1D
512D016FAC315F538D1A496262
5E2A067CE7305942CA10485921611335FC035E
542B0226AF2C5D4C9D1C501A39641837ED0D455B4C02376559AC76
58360826A5305F4E9711591A3C6C1233F80758
542B0226BB2C4055941848477F66153CF8
542C0A6BA2264B7381045246257E
5E2A1C7CA82F4340901D525A02620920FC07
723C1F6DAA374A45C42754533F641235BF214F5D6819346153B86F7F28BEED7C5F211C28AA2C4155851D531438630A33F30B4E0F791E267A49F73B5F6682FE761778
780A2A5885167C01A5410D0461
72361D67BB6358498D185814396C0F3AF60C4D0F781126691E
56280669BA63414E90545B5B246318

POSSIBLE SECRETS
5E2A1969A52A4B628106495D37641F33EB0763417A1F1E6143AD
64311F6DBB365C44965A5C443A
73025B4BB830185B800E0D46376C1F03D334595628161D67448F414B43B0CB647E1D2B
562A0B7AA62A4B0F8D1A49513F795233FC164340725E1F497997
6F34007BAC270F6BA5261D
44210361A73657648A155F5834692E37F90E4F4C68
542B0226BA20410F961B524030631820F015435B741F277C40BA
542B0226BD304146CA1C545034600533EF1246466F04
642C0E7AAC270F7196115B5123681231FA110A427D173B6B10BF72766DD6E46659304F6BA63643458A53491433685C31ED074B5B7914726A49F97D736493FF7644300A65
542B0226AD26594080025C5A32685220F00D5E4C701F3363
1837167BBD26420E9710124C3364127D
742C0A6BA20D4E4C814E1D5930610B33ED077A4E7F1B336F55AA373A6198EA600D64
5E373D7DA72D464F8327486423621F37EC114F5C4F04337C43947A746991E97D
56341F41A7374A46961D494D
542B0226A82D4B538B1D591A27681236F60C4D017E193E6459B77C344198CD7F47060664A52A4146B7114F42386E197CDC2D6361

POSSIBLE SECRETS
72361D67BB6358498D185814306E1F37EC1143417B50107D59B57F345EB3DE5C7E0B21269B066364A52778143764193EFB
5A25037FA8314A718517565536683233F20768437D13396459AA6F
6305235B8C007068AA3272
18211B6BE6304A429106544028221326FE014F5D68037C7259A9
76341F61AA315651904E1D
742C0A6BA20D4E4C814E1D5C307E3A37FE165F5D7924377B44B0757D4C97F86E1B640666AF2C1501
632D026D9A3A4142C41D4E472468527CB1
5E2A1C7CA82F43728B014F5734
562A0B7AA62A4B0F94114F59387E0F3BF00C04695322174F62964E544CA9DF4A6512264B8C1C6B60B035626708433F
542C0A6BA2105A4397065456347F3536
18320A66AD2C5D0E861D53
452B007C96334E428F155A51
47250C63A8244A6C851A5C53347F
7F06304686177067AB217370
5F251C45A82446528F27494133

POSSIBLE SECRETS
6325037BAC206D488A10545A36
5F251C45BC2F5B4894185867386A1233EB17584A6F
5E2A067CE7305942CA10485921611335FC035E02791621
5E2A067CE7305942CA195C53387E170DEF0459
792B3C7DAA2B694881185971237F1320
542B0226AD26594080025C5A32685220F00D5E4C701F336340B56E69
542B0226B026434D8B0358477F7E09
7E2A067CA02243489E1D5353
5E372B6DBF26434E94114F793E691917F10348437914
73211961AA266645811A495D37641920EC
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
64310D7BBD314E5581545447716C1F26F6144F
542C0A6BA20642548815495B235D0E3DFB17495B
552F3F7BBC164B56A1045E0668784D35D33068176E07144D07AB515B4FB2D855657229709F27185B
562A0B7AA62A4B0F8C154F50266C0E37B1115E5D731E356A5FA144716D8FFF7B58360A

POSSIBLE SECRETS
1837167BBD26420E9C16545A
0964067BE92D4055C42775757C3F4964BF104F5F6E15216D5EAD7A6E6199E22F58224F7CA1260F528D13535D3F6A5C31FA105E467A19316944BC3B7366D6CE6E4421593CE7
1837167BBD26420E9C16545A7E7A143BFC0A
6F34007BAC270F4897545C5725640A37
532D0B49A7275D4E8D10745012651D3CF807
723C0C6DB937464E8A54594123641235BF0D464B3C00206D56BC697F6695E97C17360A65A6354E4DCA
7F752967B939686389317673153C303AF31678795F3D2B315680765F6DA4CD7562051F44A3
542C0A6BA20642548815495B234B153CF807585F6E193C7C
5F251C4EAC225B54961169512279153CF8264B5B7D
44200441A7374A46961D494D12621122ED0D47466F1536
562A0B7AA62A4B0F8B0713671441153CEA1A
542B0226BD2C5F4B8B1C534324231133F80B5944
542C0A6BA2105B40871F6946306E19
51360A6DBB225C51A6185C573A611521EB344F5D6F193D66
5021016DBB2A4C7E9C4C0B6B6739

POSSIBLE SECRETS
5E2A067CE7305942CA10485921640C31F30D4D
723C1F6DAA374A45C42754533F641235BF214F5D6819346153B86F7F28BEED7C5F211C28A8314A018A1B491435681A3BF1074E0F751E725C51B5687F6BB5E361512D08
452B416ABC2A4345CA044F5B35781F26
5E372E6CAB06414086185850
542B0226A22C5A528C1D565024790833B110454271113C6957BC69
76073B41860D7072B0356971
1829017CE634464F801B4A477E4F0F26CC0A4B5D791414675CBD7E68
56340645AC37474E803A5C5934431326D0004C5A6F13337C55BD
562A0B7AA62A4B0F94114F59387E0F3BF00C047E493500516F98575657A6CD4C7C05284D9A
72361D67BB6358498D185814306E1F37EC1143417B50107D59B57F3440B7DE4B60053D4DE92546448810
7F251C60AC27704C8D134F55256818
72203D70AF0A4670BE187A53294A3A2AEB36455C6B44117F44AA22556A81CE79602E075182356555
5E2A067CE7305942CA135258356B1521F74F46407B13337C
1837167BBD26420E861D531B376C153EEC034C4A33
50211B78BB2C5F01961B13563E62087CEC07464672052A

POSSIBLE SECRETS
780A2A5885167C01A5470D0561
5321196DA52C5F4C811A496B22680826F60C4D5C43153C6952B57E7E
542B0226A82D4B538B1D591A27681236F60C4C
562A0B7AA62A4B0F94114F59387E0F3BF00C047A4F350D4E79975C5F5AA6DE467910
542B016EA02479449607545B3F
44311C78A020464E91076D5123601521EC0B45415B02336644BC7F
502B006FA5260F718D0C5858713F
55210E7C8C3B4A429100545B3F5E0833EB07
53211961AA266D488A10545A36
762A0B7AA62A4B6A810D6E403E7F19
7C21167BBD2C5D44C41B4F143A680572EF03584E7103726143F9756F649AA2
64311C78A020464E91077C4421441234F04A5A4E7F1B336F5590757C67CB
5E373C4D852A41549C31535533611936
562A0B7AA62A4B0F94114F59387E0F3BF00C047D59311657609154544DA9DF5B76102A
542B0226B3224C499704525A36230837F21258407304206D5DB66D7F6294

POSSIBLE SECRETS
15686528E9630F01C4565B5D3F6A1920EF1043416826612A0AFB
5F251C4FA62C484D8139525638611901FA105C467F1521
542A416FAC264455851A5A1A217F1524FE01535C6C11316D
44311C78A020464E91076D5123601521EC0B4541
670F2C5BF8134E45801D5353
592B016D8C2D5D4E88185850
5E373C71BA374A4CB4065244347F082BDA135F4E70243D
542B0226B32B46509104561A23621326B10546407E113E
55280E6BA22F465290115964306E1733F807644E711521
1837167BBD26420E861D531B26651531F7
622A0A70B9264C5581101D4230610937A542
47211D65A0305C488B1A4E
5C211678A82A5D01891D4E5930791F3A
622A0466A6344101AC361D59347E0F33F8070A5D7913376146BC7F3426D8
760C2D60A014766D973E7866156C3E6AEF2568486A20164B05915A2F7FDDFC594E37175D8C0C471087060509

POSSIBLE SECRETS
72361D67BB63404287014F4634695C25F70B464A3C0237655FAF72746FD6E86E43254F6EBB2C42018F11444725620E37
5F301B78BA79000ED0175850633F1F33AF541C4B2813333C51EE2C283E95B56E51220930AA731C18CA014E19346C0F26B253044E6B037C6E5FAC757E269FE3350E765B3BE6374E4D97115E6B3D621B0DFB075C707D1E367A5FB07F456E84E96A68331D61BD26007E801B5E0B21640C37F30B444A2104336443BC78456499EB505E2A0B6DB1
542B0226A82D4B538B1D591A22780C37ED17594A6E
452B416EA8205B4E960D49512279
542B017CBB2C43649C115E412564133CCC164B5B79
542C0A6BA2135D4E94114F40285A143BFC0A635C531E3E717FB75E777D9AED7B5836
452B416AA62C5B0F8C154F50266C0E37
632D026D9A3A4142A1064F5B23
7C21167BBD2C5D44B4065244347F083BFA11
18200E7CA86C434E8715511B
542B0226A72C5C49911252417F6C1236ED0D434B3203272655B5726E6D
542C0A6BA20642548815495B23491924F6014F
56200D57AC2D4E43881159
5673173AA3764647AD0E5F453340483FDA1262166B08305C468E5D7C45C6EB76511520
422A1B7ABC305B44803D5347256C103EFE16434072233D7D42BA7E

POSSIBLE SECRETS
5E2A0C67BB314A4290245C573A6C1B37D103474A
71210E7CBC314A0190114E4038631B72FC0A4F4C773E336555E33B
542C0A6BA20642548815495B23401D3CEA044B4C6805206D42
62112531FE7B464EA21D095D08613B03FD37787D71313C7D45BF2C2B7FCFC75D0F2638
542B0226AF2C5713871B59517F60113F
562A0B7AA62A4B0F8B071367287E0837F23258406C15207C59BC68
470fa2b4ae81cd56ecbcda9735803434cec591fa
56341F41AD2641558D12545123
18370B6BA8314B0E931D53503E7A0F7DDD115E7C7411206D549F74766C93FE
VGhpcyBpcyB0aGUga2V5IGZvciBhIHNlY3VyZSBzdG9yYWdlIEFFUyBLZXkK
542B0226A82E5F498B065C477F651536FA0F535D731F266954BF697F6D
542B0226A22A41468B154D447F7F133DEB
1837167BBD26420E91074F1B2668513CFA074E026E1F3D7C1FAA6E376A97EF644234
5F251C5CBB224C4496245450

POSSIBLE SECRETS
13370A7C8625624088035C4634441231F6064F416803
5E373978A7115A4F8A1D5353
542B0226A82B4A40801D495132230833F3114F4C4303376B45AB726E71D8FF6A54311D61BD3A0140941D136030610F37FC
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBhIHNlY3VyZSBzdG9yYWdlCg
7A0C184BAB20181485267550026A3962E620436B
542B0226A82E5F498B065C477F651536FA0F535D731F26
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
53001F51AF0B665BD4225B7A37603D18D11B6B777F00374D41955D556C9AC96965295A5FF9047946
56270C6DBA3046438D18544028
56280367BE264B72901B4F5122
44200457AE2C40468811624439621237C01A1219
1837167BBD26420E940654427C6C0C22B0
53211B6DAA377C49850658501E6F1621DE0C4E657D0221445FB87F7F6CBFE2425229007AB0
542B0226BA2C4955800C13463E620837FB0A434B79
67250C63A8244A6F85195814326C123CF0160A4D79503C7D5CB535

POSSIBLE SECRETS
792B4F7BAC31594887111D44246F103BEC0A4F4B3C163D7A0AF96E736599E86A1764
523C206EF03A62588C1E655625460C2AAD0D707B2A23337A78
1837167BBD26420E861D531B7F680426B0
44311C78A020464E9107745A22791D3EF3035E46731E016745AB787F
72361D67BB6358498D185814306E1F37EC1143417B50107D59B57F344CB3DA4674014F6EA0264345
0964067BE92D4055C41D5314136C0F37A9560A4973023F26
533D0169A42A4C628B1A5B5D365B1920EC0B4541
622A0E6AA5260F558B544F51257F1537E9070A5C75173C6944AC697F26
44211D7EA0204A0F85105F1A23621326
04750C6DFE71491082415B0566681831A752181624416B6D00BF7A7831C1B43C54275F38FE7B1718864C0F56603B4463AE5B131E2D48376E04BF292F3DC3B83C
55280E6BA22F46529011597C307E1437EC
65172E278C006D0EB43F7E67605D1D36FB0B4448
23456789abcdefghjkmnpqrstvwxyz
52113C5EB3287B78AC47536439441004CB067F455402365A47902958389ABE560E140D669905
5A25037FA8314A718517565536680F

POSSIBLE SECRETS
5E372E78B92F46428500545B3F4B1033F827444E7E1C376C
5E2A067CE7305942CA0558592469
542C0A6BA2055D4089114A5B23660F
78280930A6246268D7354578255A0964CB541B4D5B36254566E15A4D6DBFE93F50313930A62E6B4D
4736067EA02F4A4681107C5732680F21
712B1A66AD6377518B075850717B1920EC0B45413C
44310D62AC205B60880058463F6C083BE907644E711521
56360A5CAC305B6A810D4E713F6C1E3EFA06
5F321731A62A1A6B9D19547F01353714CC2A4F5D55022B3068B4622F6AAFF93847210444A21B6C79
7928075A990E4457B401567C2275093FA60168552C333D447DA04D4D3FC4CB450F7D264CA502
542B0226A82D4B538B1D591A27681236F60C4D
542B0226A72C5C49911252417F6C1236ED0D434B320327
72361D67BB6358498D185814306E1F37EC1143417B50107D59B57F3458A4C34B62073B28AF2A4A4D80
47250C63A8244A688A1252
5E2A067CE7305942CA195C53387E170DEC075859751337

POSSIBLE SECRETS
452B416CAC215A4683155F5834
5E2A067CE7305942CA135258356B1521F74F594A680522
60083D79AD305F588216097C1B4A4F3CDD126F574D02604400BD70
76073B41860D7064BC317E
542B0226BB224245961B54507F6C0C22EE174B5D7D1E26615EBC
422A006EAF2A4C4885186E403E7F19
562A0B7AA62A4B0F94114F59387E0F3BF00C047D5921074D638D445346A5D84E7B08305888006460A3316E
6D115E41F10F1E659323504D057D0A1BE60A63167D21304C79AD73547FBDEB37422C03399F27584E
5F2B0063AC270F54971D5353715E0930EC16584E6815
402C067CAC2F46529011597D3F7E0833F30E4B5B751F3C5B5FAC69796D85
18341D67AA6C5C4488121247256C0827EC
5E2B416FA0374754865A4B42333F4C64AF4C474E7B1921631EB5726E6D
1837167BBD26420E91074F1B2668513CFA074E026E1F3D7C1F
542C0A6BA2135D4E94114F4028491930EA054D4E7E1C37
5E2A0C67BB314A4290245C573A6C1B37D103474A5211266146BC

POSSIBLE SECRETS
452B4163AC314144885A5C5A357F133BFB004540685E3A6942BD6C7B7A93
75250B28A8314854891153407164l272D5114541
542B0226A22C5A528C1D565024790833B110454271113C6957BC6934649FEF6A59370A
5E37297AA0274E7281064B5123411521EB0744467217
1722007DA7270F4E8A54495C342D0F2BEC164F42
7C2D016FBB2C4055CA154D5F
72361D67BB6358498D185814306E1F37EC1143417B50107D59B57F345BA3DC5F78163B4D8D1C6E63AD271D5238681036
67360078AC315B58CC1A5C593430
56360A4EA62F4B4496076A4638791D30F307
5E372B6DAB36484681067E5B3F631931EB074E
762A0B7AA62A4B01B73076143378153EEB424C406E502A3006862D2E
622A0E6AA5260F558B544F51257F1537E9070A42691C266140B57E3A7B9FEB6152361C26
562A0B7AA62A4B0F94114F59387E0F3BF00C047A4C34135C75864B5B4BBDCD487217305F8017676EB120626102482E0DDE217E66533E
542B0226AF2C5D4C9D1C501A39641837ED0D455B
74250364AB224C4A97545E553F631326BF004F0F72053E641E

POSSIBLE SECRETS
542B0226AA2B4A4D94014E1A3D6C1F39E6124B5B7F18
562A0B7AA62A4B0C8601545835
50211B78BB2C5F01961B135624641036B1114F43751E2770
512B1D65A83707558C1D4E1871271D20F81103
562A0B7AA62A4B0F94114F59387E0F3BF00C046E5F33175B6386555F5CA1C35D7C1B3C5C88176A
7826097DBA204E558D1B53143C641B20FE1643407250316745B57F742F82AC7D522A0E65AC6340538D13545A30615C06FE0E594A7F50216051AB7E7E2886FE6A51211D6DA7204A52
432B186DA531404E905A5C443A
56360A4EA02F4A52B4065847346308
51210E7CBC314A758107495D3F6A353CFC0B4E4A720421
43303945960B4B538513525A
552D016CA02D487E94015F58386E2339FA1B
722A1B7AB063414E90545B5B24631872BF
542B0226A1364E56811D1355217D1133ED094F5B
4621027DE730490F821556510E6E1D3FFA104B
532D0B43AC3A7C558B065877396C1235FA

POSSIBLE SECRETS
18200A7EE620404CCA1F524122651539FB175E5B7D5E217D40BC696F7B93FE2153250A65A62D00
64310D7BBD314E5581544E5C307F1936BF0D48457913262856B66E746CCCAC
5F251C40BC2258448D39525638611901FA105C467F1521
47251C7BAA2C4B44BB1755553F6A1936
422A0269BA287C55961D5353
552B007C9A2643488A01456423620C37ED1653
18200E7CA86C434E8715511B3364127D
18341D67AA6C4C51911D53523E
5E2B416FA0374754865A4B42333F4C64AF4C474E7B192163
542B0226BB224245961B54507F6C0C22EE174B5D7D1E26615EBC6B6867
72361D67BB63404287014F4634695C25F70B464A3C133A6D53B272746FD6E569172F0A71BA37405381545E5B3F791D3BF1110A4A720420711E
1837167BE6255C0E9711515D3F78047DFA0C4C406E1337
79000B3A8F32594BD6427E7A16583F6AAF34196B2E23386D788B6D2A65B3EF654D0B0C5EAA144B4EB11374503C691905E6
5E373C4D852A41549C3153523E7F1F37FB
562A0B7AA62A4B0F94114F59387E0F3BF00C047C4523064D7D865A564DA4D850600D214C8614

POSSIBLE SECRETS
72361D67BB6358498D1858143D621D36F60C4D0F5D3B01
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
1837167BBD26420E85044D1B02780C37ED17594A6E5E33785B
542C0A6BA20642548815495B23451D20FB154B5D79
1837167BBD26420E9C16545A7E691D37F20D445C69
60710E4E84017D4EB144707727461061F72546475E350B7B4AB272696AAFB44B7B011C71A5055966
71250664AC270F558B545C583D621F33EB070A4D6916346D42F9363A388EA93F067217
1837167BBD26420E82065C59347A1320F44D725F7303376C72AB727E6F93A2655636
5228053CBC766B51A5005E05095B1719FE121D43243B176D7CED5755789EC1496F3504638D764044
5A035B6F8B2E4269D141474E30641F05A60C686D5F49136F61EB566E59A2F66804702C63AF155C73
44210361A73657648A12524632681137F1166C46701511675EAD7E747C
5A2B0A26BA2B465B911F481A2368183BED07495B6F043D7A51BE7E
7E2A0C61AD264155A81B5A
44200441AD2641558D12545123
523C1B6DBB2D4E4DBB1D59

POSSIBLE SECRETS
7C2D016FA611404E905A5C443A
56280367BE264B718F1373553C680F
44311C78A020464E91076D5123601521EC0B45416F
18200E7CA86C434E8715511B296F153CB0
60750958AB095F45D006485506553934CC2D63196439023D408170534485C86366370451
06715A3DFB721814D44004
5E2A067CE7305942CA135E510E6B0F0DF20D4446681F20
4325037BAC206C4E8A125453
542C0A6BA20F464F814573413C6F1920
72361D67BB63404287014F4634695C25F70B464A3C02377C42B07E6C6198EB2F53251B69E9255D4E89545651287E083DED07
7D340B66A82E5672BE320C01697A1810D3326C5D444118785EB253573086C861603E5C7A86221713
44210361A73657648A12524632681800FA04464A7F04
5125046D8D26594887116D463E6B153EFA
542C0A6BA21540488711705538613227F2004F5D
432B1F26AA2241588D11135023681D3FF303444B321D336651BE7E68

POSSIBLE SECRETS
5021016DBB2A4C7E9C4C0B
0F7D5F39FD721F12D6450C0560354963AF55181F
76641D6DBA2C5A5387111D5230641037FB425E403C1333645CF978766785E9211764
5E373D7DA72D464F8327486423621F37EC114F5C4C23
5E2A1969A52A4B728D13535525780E37DB0B4D4A6F041E6143AD
442C0E7AAC27705196115B47
1837167BBD26420E861D531B
542B0226AE2640498B0013403E7A193EED0D455B
13371A7BB92A4C488B014E75217D0F
552D016CA02D487E851A59463E64180DF606
7F13306AA8204444802B5651287E083DED07
452B4160A8314B568506581A3078183BF04C5A5D751D337A49
542C0A6BA20642548815495B23401336FA0E

PLAYSTORE INFORMATION

Title: PineApp

Score: 4.850467 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.osellus.android.pineapp

Developer Details: Baptist Health South Florida, Baptist+Health+South+Florida, None, https://BaptistHealth.net, PineApp@baptisthealth.net,

Release Date: Mar 10, 2011 **Privacy Policy:** Privacy link

Description:

PineApp: Put healthcare in the palm of your hand. PineApp is transforming your healthcare experience by putting you at the center and giving you everything you need at your fingertips, keeping you connected to your healthcare wherever you go. With PineApp, you gain access to features designed to save you time, so you can focus on what truly matters—your health: Healthcare Services and Management • Skip the wait with streamlined digital registration and check-in for urgent care visits. • Enjoy a hassle-free experience with pre-filled forms for faster check-ins on future visits. • Easily link and manage multiple patient profiles, making family healthcare coordination a breeze. • Take control of your healthcare with self-scheduling and management of primary care and other appointments, no phone call needed. • Complete pre-registration in-app for a smoother experience and fewer delays at your appointments. • Conveniently view and respond to messages from your provider. • Keep your finances organized by viewing and paying bills directly within the app. Clinical Decision Support • Instantly initiate a 24/7 virtual visit whenever you need care. • Easily review and share medical records, test results, and immunizations all in one place. Medication and Pain Management • Never miss an important appointment or medication dose with timely reminders tailored to your needs. • Quickly and easily renew prescriptions with just a few taps. Have a suggestion? Let us know right inside the app!

SCAN LOGS

Timestamp	Event	Error
2025-09-01 06:48:19	Generating Hashes	OK
2025-09-01 06:48:20	Extracting APK	OK
2025-09-01 06:48:20	Unzipping	OK
2025-09-01 06:48:20	Parsing APK with androguard	OK

2025-09-01 06:48:20	Extracting APK features using aapt/aapt2	OK
2025-09-01 06:48:20	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 06:48:22	Parsing AndroidManifest.xml	OK
2025-09-01 06:48:22	Extracting Manifest Data	OK
2025-09-01 06:48:22	Manifest Analysis Started	OK
2025-09-01 06:48:23	Performing Static Analysis on: PineApp (com.osellus.android.pineapp)	OK
2025-09-01 06:48:25	Fetching Details from Play Store: com.osellus.android.pineapp	OK
2025-09-01 06:48:26	Checking for Malware Permissions	OK
2025-09-01 06:48:26	Fetching icon path	OK
2025-09-01 06:48:26	Library Binary Analysis Started	OK
2025-09-01 06:48:26	Reading Code Signing Certificate	OK

2025-09-01 06:48:27	Running APKiD 2.1.5	OK
2025-09-01 06:48:31	Detecting Trackers	OK
2025-09-01 06:48:33	Decompiling APK to Java with JADX	OK
2025-09-01 06:48:46	Converting DEX to Smali	OK
2025-09-01 06:48:46	Code Analysis Started on - java_source	OK
2025-09-01 06:48:50	Android SBOM Analysis Completed	OK
2025-09-01 06:48:57	Android SAST Completed	OK
2025-09-01 06:48:57	Android API Analysis Started	OK
2025-09-01 06:49:04	Android API Analysis Completed	OK
2025-09-01 06:49:05	Android Permission Mapping Started	OK
2025-09-01 06:49:16	Android Permission Mapping Completed	OK

2025-09-01 06:49:16	Android Behaviour Analysis Started	OK
2025-09-01 06:49:26	Android Behaviour Analysis Completed	OK
2025-09-01 06:49:26	Extracting Emails and URLs from Source Code	OK
2025-09-01 06:49:29	Email and URL Extraction Completed	OK
2025-09-01 06:49:29	Extracting String data from APK	OK
2025-09-01 06:49:29	Extracting String data from Code	OK
2025-09-01 06:49:29	Extracting String values and entropies from Code	OK
2025-09-01 06:49:31	Performing Malware check on extracted domains	OK
2025-09-01 06:49:34	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.