ANDROID STATIC ANALYSIS REPORT

app_icon

PillEye (3.2.0)

File Name:	com.rocateer.mediscount_551.apk
Package Name:	com.rocateer.mediscount
Scan Date:	Sept. 1, 2025, 8:15 a.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	16	3	1	1

FILE INFORMATION

File Name: com.rocateer.mediscount_551.apk
Size: 33.18MB
MD5: 2541b156c66001f181f94a36c14c9147
SHA1: 6250aaf27eceb428bab30239c1006e0282065d5a
SHA256: 7791bbc1aa1b211c0fbb6b675e71c6fb53cba2194bfcb6b19469f879d37a2e23

APP INFORMATION

App Name: PillEye
Package Name: com.rocateer.mediscount
Main Activity: com.rocateer.mediscount.MainActivity
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 3.2.0

Android Version Code: 551

APP COMPONENTS

Activities: 10
Services: 8
Receivers: 6
Providers: 6
Exported Activities: 0
Exported Services: 0
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-11-05 06:02:21+00:00
Valid To: 2050-11-05 06:02:21+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x32eef66c77980d57a9d69ea4a60eff65a7fe639
Hash Algorithm: sha256
md5: 127f12b40efe01db4cb047c77ef8c41a
sha1: a68e1f7e5cd6d3255e72139da8963410e6495832
sha256: a8421cdd239873a2c5db53be85156a3a081e09ff5815803b41bbe75299490c5b
sha512: ce17b13b574642368df2674b0e74a0fbd1dc84793525b1b04836080c087731cae9435f6c6b2e563e923197075a46f3cbe2b802da5d4c8b421e3b88536421dfb8
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: c75a9d594dc274ad7c1bef6ff2854f47113160130936282256ad1a44eceb6be4
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.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.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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

PERMISSION	STATUS	INFO	DESCRIPTION
com.rocateer.mediscount.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check</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</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.rocateer.mediscount.MainActivity	Schemes: http://, https://, Hosts: pilleye.com, Path Prefixes: /applink,

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: **4** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Broadcast Receiver (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.
4	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
5	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: **0** | WARNING: **8** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b7/a.java ba/b.java c/d.java c5/f.java c5/n.java c6/b.java c6/c.java c6/i.java c6/r.java c6/t.java c6/v.java c6/y.java c6/z.java c7/a.java ca/a.java ca/b.java com/pichillilorenzo/flutter_inappwebview_android

NO	ISSUE	SEVERITY	STANDARDS	FILES
				/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/InAppWebViewChromeClient.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebViewClient.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebViewClientCompat.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebViewRenderProcessClient.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InputAwareWebView.j

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	ava com/rocateer/mediscount/MainActivity.java d6/f.java d6/i.java d6/j.java d6/m.java d6/t.java d6/x.java da/d.java da/e.java da/h.java e8/e.java ea/f.java f1/e.java f7/h.java f9/b.java g2/o.java g6/d.java g6/e0.java g6/k0.java g6/u.java g6/x.java g9/c.java h0/a0.java h1/l.java h5/a.java ia/c0.java ia/e0.java ia/i.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundService.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingReceiver.java io/flutter/plugins/firebase/messaging/b.java io/flutter/plugins/firebase/messaging/i.java io/sentry/android/core/u.java io/sentry/android/replay/s.java io/sentry/android/replay/v.java io/sentry/flutter/SentryFlutter$updateOptions$24.java io/sentry/flutter/SentryFlutterPlugin.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/sentry/flutter/SentryFlutterPlugin.java io/sentry/flutter/SentryFlutterReplayRecorder.java io/sentry/r6.java j0/d.java k1/d.java k5/a.java k5/q.java k5/s.java k5/u.java l6/b.java la/d.java lb/b6.java lb/k6.java m6/e.java m6/n.java mb/a.java n1/c.java o8/e.java ob/g0.java p5/k.java p6/b.java pb/j.java qb/a.java qb/e0.java r8/g.java r8/o.java r9/m.java rb/j.java s5/a.java u/y0.java u7/d.java ua/b.java v0/b.java v4/a.java v7/b.java w/s0.java w9/n.java w9/p.java x2/l.java x4/q.java x7/g.java y1/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				y1/a.java z0/f.java z4/a.java z4/e.java
2	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/pichillilorenzo/flutter_inappwebview_android/credential_database/CredentialDatabaseHelper.java ia/i.java w5/m0.java w5/t0.java
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/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 h2/a.java qb/d0.java
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	a3/d1.java l2/r1.java lc/a.java lc/b.java mc/a.java n2/b.java
5	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	f9/b.java io/sentry/util/u.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	f9/c.java lb/p7.java lb/w5.java w/u.java
7	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	e8/s.java io/sentry/android/core/internal/util/n.java
8	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	io/flutter/plugin/editing/b.java io/flutter/plugin/platform/g.java
9	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	io/sentry/android/core/s0.java pb/i.java pb/j.java
10	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/n.java
11	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	w2/c.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	io/sentry/android/core/cache/b.java io/sentry/android/core/s0.java io/sentry/android/core/z.java io/sentry/android/replay/capture/f.java io/sentry/android/replay/g.java io/sentry/cache/b.java io/sentry/cache/c.java io/sentry/cache/e.java io/sentry/flutter/SentryFlutterReplayRecorder.java io/sentry/p.java io/sentry/p5.java io/sentry/u2.java io/sentry/w.java io/sentry/w2.java l0/s0.java lb/w5.java p1/m.java pb/j.java w/u.java ya/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/pichillilorenzo/flutter_inappwebview_android/Util.java f9/c.java fc/j.java i2/d.java i2/w.java io/sentry/android/core/SentryPerformanceProvider.java io/sentry/android/replay/g.java io/sentry/cache/b.java io/sentry/cache/c.java io/sentry/cache/e.java io/sentry/config/e.java io/sentry/u2.java io/sentry/util/e.java io/sentry/w.java io/sentry/w2.java p1/m.java w/u.java
00096	Connect to a URL and set request method	command network	com/pichillilorenzo/flutter_inappwebview_android/Util.java g9/c.java i2/m.java io/sentry/transport/o.java
00089	Connect to a URL and receive input stream from the server	command network	g9/c.java i2/m.java io/sentry/transport/o.java
00030	Connect to the remote server through the given URL	network	com/pichillilorenzo/flutter_inappwebview_android/Util.java i2/m.java io/sentry/transport/o.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	g9/c.java i2/m.java io/sentry/transport/o.java
00094	Connect to a URL and read data from it	command network	com/pichillilorenzo/flutter_inappwebview_android/Util.java i2/m.java
00108	Read the input stream from given URL	network command	i2/m.java
00014	Read file into a stream and put it into a JSON object	file	f9/c.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	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 d6/g.java k5/a.java k5/q.java k5/u.java la/d.java rb/i.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserManager.java d6/g.java k5/a.java k5/q.java k5/u.java rb/i.java
00012	Read data and put it into a buffer stream	file	io/sentry/cache/b.java io/sentry/cache/e.java io/sentry/config/e.java io/sentry/u2.java io/sentry/util/e.java io/sentry/w.java
00123	Save the response to JSON after connecting to the remote server	network command	com/pichillilorenzo/flutter_inappwebview_android/Util.java
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
00132	Query The ISO country code	telephony collection	g2/i0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java d6/g.java i2/w.java k5/a.java k5/q.java la/d.java
00202	Make a phone call	control	k5/u.java
00203	Put a phone number into an intent	control	k5/u.java
00028	Read file from assets directory	file	i2/a.java
00161	Perform accessibility service action on accessibility node info	accessibility service	h1/l.java io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/e.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	h1/l.java io/flutter/view/AccessibilityViewEmbedder.java
00003	Put the compressed bitmap data into JSON object	camera	com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebView.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebViewChromeClient.java f2/a.java
00209	Get pixels from the latest rendered image	collection	io/flutter/embedding/android/j.java

RULE ID	BEHAVIOUR	LABEL	FILES
00210	Copy pixels from the latest rendered image into a Bitmap	collection	io/flutter/embedding/android/j.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://mediscount-36e05.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/900149314892/namespaces/firebase:fetch?key=AIzaSyACDXsXoIdKbDI61nEZbFhRJTgFytv1afA is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'is_documents_cleanup_enabled': 'true'}, 'state': 'UPDATE', 'experimentDescriptions': [{'experimentId': '_exp_rollout_5', 'variantId': '1', 'experimentStartTime': '2025-07-28T00:56:32.595709Z', 'triggerTimeoutMillis': '15552000000', 'timeToLiveMillis': '15552000000'}], 'templateVersion': '25', 'rolloutMetadata': [{'rolloutId': 'rollout_5', 'variantId': '1', 'affectedParameterKeys': ['is_documents_cleanup_enabled']}]}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.INTERNET, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	1/44	com.google.android.c2dm.permission.RECEIVE

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.

DOMAIN	STATUS	GEOLOCATION
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
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:** 140.82.113.3 **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

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
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
mediscount-36e05.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
dashif.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
aomedia.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
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:** 17.253.83.135 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
default.url	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.example.com	ok	**IP:** 23.220.73.43 **Country:** Colombia **Region:** Antioquia **City:** Medellin **Latitude:** 6.251840 **Longitude:** -75.563591 **View:** Google Map

✉ EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	d6/s.java

TRACKERS

TRACKER	CATEGORIES	URL
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://mediscount-36e05.firebaseio.com"
"google_api_key" : "AIzaSyACDXsXoIdKbDI61nEZbFhRJTgFytv1afA"
"google_crash_reporting_api_key" : "AIzaSyACDXsXoIdKbDI61nEZbFhRJTgFytv1afA"
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
9a04f079-9840-4286-ab92-e65be0885f95
e2719d58-a985-b3c9-781a-b030af78d30e

PLAYSTORE INFORMATION

Title: PillEye – tablet, pill counter

Score: 4.03 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.rocateer.mediscount

Developer Details: Medility, 9130297786965025644, None, https://pilleye.com, help@pilleye.com,

Release Date: Dec 9, 2020 **Privacy Policy:** Privacy link

Description:

With the pill counter, Pilleye, you can count pills, tablets in the blink of an eye just by taking a picture! How many times do you count your pills per day? What if you need to answer the phone while counting pills? Are you worried about the pills you counted are not correct? Pilleye is here to help you to solve all these problems in your pharmacy. Stop the hassle of counting tablets by hand. The pill counter with accuracy, from now on 'Enjoy your counting!' Pilleye is, -Accurate: Over 99.99% accuracy is shown. -Versatile: It is not limited to round tablets, but can count pills and capsule of all shapes and sizes. -Time saving: You can count 500 tablets, capsules in just 1 second. 50 times faster than hand. With this pill counter, you can effectively reduce the amount of time spent on inventory checks. -Record storage: You can store all the records in Pilleye. Pilleye will reduce unnecessary arguments with patients about a miscount.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 08:15:56	Generating Hashes	OK
2025-09-01 08:15:57	Extracting APK	OK
2025-09-01 08:15:57	Unzipping	OK
2025-09-01 08:16:06	Parsing APK with androguard	OK
2025-09-01 08:16:06	Extracting APK features using aapt/aapt2	OK

2025-09-01 08:16:06	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 08:16:09	Parsing AndroidManifest.xml	OK
2025-09-01 08:16:09	Extracting Manifest Data	OK
2025-09-01 08:16:09	Manifest Analysis Started	OK
2025-09-01 08:16:09	Performing Static Analysis on: PillEye (com.rocateer.mediscount)	OK
2025-09-01 08:16:10	Fetching Details from Play Store: com.rocateer.mediscount	OK
2025-09-01 08:16:12	Checking for Malware Permissions	OK
2025-09-01 08:16:12	Fetching icon path	OK
2025-09-01 08:16:12	Library Binary Analysis Started	OK
2025-09-01 08:16:12	Reading Code Signing Certificate	OK
2025-09-01 08:16:13	Running APKiD 2.1.5	OK

2025-09-01 08:16:19	Detecting Trackers	OK
2025-09-01 08:16:21	Decompiling APK to Java with JADX	OK
2025-09-01 08:16:52	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 08:16:52	Decompiling classes2.dex with JADX	OK
2025-09-01 08:16:59	Decompiling classes.dex with JADX	OK
2025-09-01 08:17:22	Decompiling with JADX failed for classes.dex	OK
2025-09-01 08:17:22	Decompiling classes2.dex with JADX	OK
2025-09-01 08:17:28	Decompiling classes.dex with JADX	OK
2025-09-01 08:18:23	Some DEX files failed to decompile	OK
2025-09-01 08:18:23	Converting DEX to Smali	OK
2025-09-01 08:18:23	Code Analysis Started on - java_source	OK

2025-09-01 08:18:30	Android SBOM Analysis Completed	OK
2025-09-01 08:18:42	Android SAST Completed	OK
2025-09-01 08:18:42	Android API Analysis Started	OK
2025-09-01 08:18:54	Android API Analysis Completed	OK
2025-09-01 08:18:55	Android Permission Mapping Started	OK
2025-09-01 08:19:04	Android Permission Mapping Completed	OK
2025-09-01 08:19:04	Android Behaviour Analysis Started	OK
2025-09-01 08:19:15	Android Behaviour Analysis Completed	OK
2025-09-01 08:19:15	Extracting Emails and URLs from Source Code	OK
2025-09-01 08:19:26	Email and URL Extraction Completed	OK

2025-09-01 08:19:26	Extracting String data from APK	OK
2025-09-01 08:19:26	Extracting String data from Code	OK
2025-09-01 08:19:26	Extracting String values and entropies from Code	OK
2025-09-01 08:19:32	Performing Malware check on extracted domains	OK
2025-09-01 08:19:36	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.