MOBSF

ANDROID STATIC ANALYSIS REPORT

Kindroid (1.27)

File Name:	kindroid-1-27.apk
Package Name:	com.kindroid.app
Scan Date:	April 14, 2024, 1:28 a.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	16	1	1	1

FILE INFORMATION

File Name: kindroid-1-27.apk
Size: 6.96MB
MD5: c675982ed01eb91ecf9c15e30a76dd2f
SHA1: 841b3733fa83dafb98301535aa8b3be9e1e90a34
SHA256: a2c3539f9a9bcbd9e07b35d00ba507b7f3fe757e25cce6a5d9a7ccc6a910ba15

APP INFORMATION

App Name: Kindroid
Package Name: com.kindroid.app
Main Activity: com.kindroid.app.MainActivity
Target SDK: 33
Min SDK: 23
Max SDK:
Android Version Name: 1.27

Android Version Code: 27

APP COMPONENTS

Activities: 8
Services: 6
Receivers: 4
Providers: 3
Exported Activities: 2
Exported Services: 1
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2023-06-26 01:29:16+00:00
Valid To: 2053-06-26 01:29:16+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x91959ea70d570d14b95fc32e10df8a7a28c2728
Hash Algorithm: sha256
md5: 6f346793c8a12c3d213d110c8f404d5b
sha1: 0afed57c4b82741d504d53f5a5dff78a2d716f29
sha256: 241b6ba4c1e4e5908de12ed1b6b3ed364569479df79f2fa34982b0aeea48c29b
sha512: 1862ab7ee175e6beb8a350be862f55da07506050cd68f9839e8d971dae2a5b105ee44b964b92eb357c2530562078faac614d395b16608f519dc7a9ec00fe9d9d
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 3ccde60fce29328e480243da97fc677e355e41e021b47f1e50eaf690e8c538e3
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.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.kindroid.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.BRAND check
Build.DEVICE check
Build.BOARD check
Build.TAGS check</td></tr>
<tr><td>Obfuscator</td><td>Kiwi encrypter</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></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>

FILE	DETAILS
classes3.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.kindroid.app.MainActivity	Schemes: https://, Hosts: kindroid.page.link,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 7 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched 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.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Activity (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Activity (com.google.firebase.auth.internal.RecaptchaActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
6	Broadcast Receiver (com.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
7	Broadcast Receiver (com.amazon.device.iap.ResponseReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.amazon.inapp.purchasing.Permission.NOTIFY [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
8	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: **6** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/getcapacitor/AppUUID.java com/getcapacitor/Bridge.java com/getcapacitor/Plugin.java com/revenuecat/purchases/amazon/AmazonBillingKt.java com/revenuecat/purchases/amazon/AmazonCacheKt.java com/revenuecat/purchases/common/BackendKt.java com/revenuecat/purchases/common/caching/DeviceCache.java com/revenuecat/purchases/common/diagnostics/DiagnosticsEntry.java com/revenuecat/purchases/common/diagnostics/DiagnosticsSynchronizer.java com/revenuecat/purchases/common/diagnostics/DiagnosticsTracker.java com/revenuecat/purchases/common/offlineentitlements/ProductEntitlementMapping.java com/revenuecat/purchases/common/verification/DefaultSignatureVerifier.java com/revenuecat/purchases/strings/ConfigureStrings.java com/revenuecat/purchases/subscriberattributes/SubscriberAttribute.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java io/capawesome/capacitorjs/plugins/firebase/authentication/FirebaseAuthenticationHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/amazon/a/a/g/d.java com/amazon/a/a/o/c.java com/amazon/c/a/a/d.java com/amazon/device/drm/LicensingService.java com/amazon/device/drm/a/d/c.java com/amazon/device/iap/PurchasingService.java com/amazon/device/iap/internal/c/e.java com/amazon/device/simplesignin/BroadcastHandler.java com/amazon/device/simplesignin/SimpleSignInService.java com/amazon/device/simplesignin/a/c/b.java com/capacitor/rateApp/CapacitorRateApp.java com/capacitorjs/plugins/network/NetworkPlugin.java com/getcapacitor/Logger.java com/getcapacitor/plugin/CapacitorCookieManager.java com/pantrist/firebase/dynamiclinks/CapacitorFirebaseDynamicLinks.java com/revenuecat/purchases/common/DefaultLogHandler.java com/revenuecat/purchases/hybridcommon/mappers/PurchasesPeriod.java io/capawesome/capacitorjs/plugins/firebase/authentication/handlers/AppleAuthProviderHandler.java io/capawesome/capacitorjs/plugins/firebase/authentication/handlers/FacebookAuthProviderHandler.java io/capawesome/capacitorjs/plugins/firebase/authentication/handlers/GoogleAuthProviderHandler.java io/capawesome/capacitorjs/plugins/firebase/authentication/handlers/OAuthProviderHandler.java io/capawesome/capacitorjs/plugins/firebase/authentication/handlers/PlayGamesAuthProviderHandler.java
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/amazon/a/a/o/b/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/amazon/a/a/o/b/a.java com/revenuecat/purchases/common/UtilsKt.java
5	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/amazon/device/drm/LicensingService.java com/amazon/device/iap/PurchasingService.java
6	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/amazon/a/a/b/b.java com/amazon/a/a/i/b.java com/amazon/a/a/l/c.java
7	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/capacitorjs/plugins/filesystem/Filesystem.java com/getcapacitor/BridgeWebChromeClient.java com/getcapacitor/FileUtils.java
8	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/getcapacitor/BridgeWebChromeClient.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/24	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.RECORD_AUDIO, android.permission.CAMERA, android.permission.WAKE_LOCK
Other Common Permissions	2/45	android.permission.MODIFY_AUDIO_SETTINGS, 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
rev.cat	ok	**IP:** 52.72.49.79 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
errors.rev.cat	ok	**IP:** 67.199.248.13 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
docs.revenuecat.com	ok	**IP:** 3.162.3.113 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.amazon.com	ok	**IP:** 3.161.255.150 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api.revenuecat.com	ok	**IP:** 54.86.220.248 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
play.google.com	ok	**IP:** 172.217.13.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api-diagnostics.revenuecat.com	ok	**IP:** 54.86.220.248 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
capacitorjs.com	ok	**IP:** 172.64.80.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AIzaSyCpMpa1EO6C5BM3B_dGEFZLOcinb6FGLME"
"google_crash_reporting_api_key" : "AIzaSyCpMpa1EO6C5BM3B_dGEFZLOcinb6FGLME"
115792089210356248762697446949407573529996955224135760342422259061068512044369
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

POSSIBLE SECRETS
UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMlM=
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
115792089210356248762697446949407573530086143415290314195533631308867097853951
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n

POSSIBLE SECRETS

PLAYSTORE INFORMATION

Title: Kindroid: AI Companion Chat

Score: 4.552381 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Entertainment **Play Store URL:** com.kindroid.app

Developer Details: Kindroid, 8268215859556130436, 5551 Hollywood Blvd #1277 Los Angeles, CA 90028, https://kindroid.ai, hello@kindroid.ai,

Release Date: Jul 28, 2023 **Privacy Policy:** Privacy link

Description:

Kindroid enables you to build a digital friend so realistic, it feels like conversing with a human. Welcome to a world where cutting-edge AI blends seamlessly with human empathy. Create Your Unique AI Friend - With Kindroid, you get to shape your AI's personality. Craft a detailed backstory and implant key memories, making your AI genuinely one-of-a-kind. Whether you want a friend to chat with, a character for roleplay, or a digital confidant, Kindroid's sophisticated language learning model (LLM) ensures your AI is as unique as you are. Engage in Dynamic Conversations - Dive into deep, meaningful, or fun conversations with your AI. From discussing the latest news, sharing a romantic moment, to exploring complex topics, Kindroid's AI adapts to your conversational style. It's not just an app; it's a companion that grows and learns from every interaction. See Your Kindroid Come to Life - Visualize your AI companion like never before. Through diffusion-generated selfies, Kindroid provides a visual representation of your AI, adding a new dimension to your interaction. Each image is a unique creation, reflecting the personality and essence of your AI friend. Experience Real-Time Voice Calls - Kindroid takes interaction to the next level with real-time voice calls. Engage in conversations using state-of-the-art audio transcription technology, making your conversation more spontaneous and lively. Kindroid also offers best-in-class text-to-speech capabilities, allowing your AI to sound incredibly human-like. Unparalleled Connectivity - Kindroid isn't just confined to the app. Your AI companion can access the internet, view links, and see images, enriching conversations with up-to-date information and visual context. This feature adds an extra layer of immersion, making your interactions with your AI friend more dynamic and informative. Why Choose Kindroid? * Sophisticated AI: Powered by an advanced language learning model, Kindroid offers realistic, engaging conversations. * Customizable Companions: Create an AI that resonates with your personality and preferences. * Visual Interaction: See your AI through unique, diffusion-generated selfie images. * Voice Communication: Talk to your AI in real-time with state of the art voice transcription. * Internet-Connected: Discuss current events, share links, and let your Kindroid see images for a more immersive experience. Join Our Community - Engage with other Kindroid users, share experiences, and get inspired. Whether you're into roleplaying, looking for a text game adventure, or seeking a unique friend, our community is welcoming and diverse. Come join our growing community of Kindroid lovers on Discord, Reddit, and Facebook: https://discord.gg/kindroid https://www.reddit.com/r/KindroidAI/ https://www.facebook.com/groups/kindroid Continual Updates & Support - We believe in constant improvement. Regular app updates ensure a seamless experience, introducing new features and enhancements based on user feedback. Download Kindroid Today! - Begin your journey with the most advanced AI companion app on the market. Create your AI, engage in fascinating conversations, and explore the world with your Kindroid. For help: contact hello@kindroid.ai Legal terms & privacy: https://kindroid.ai/legal

Report Generated by - MobSF v3.9.8 Beta

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.