MOBSF

ANDROID STATIC ANALYSIS REPORT

Clue (185.0)

File Name:	com.clue.android_3083.apk
Package Name:	com.clue.android
Scan Date:	Aug. 29, 2025, 9:11 p.m.
App Security Score:	57/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	17	3	3	1

FILE INFORMATION

File Name: com.clue.android_3083.apk
Size: 16.34MB
MD5: be4eb2c2c7fa09cd585a5c002134db57
SHA1: 3d6c7d303441f2234a384a15064ffe9d9b43804b
SHA256: 88566a90d30e3efe4e3711e928e6ec8e9c8164d292033b115a7d59e09270a5f3

APP INFORMATION

App Name: Clue
Package Name: com.clue.android
Main Activity: com.helloclue.ui.MainActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 185.0

Android Version Code: 3083

APP COMPONENTS

Activities: 12
Services: 11
Receivers: 15
Providers: 2
Exported Activities: 3
Exported Services: 1
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: O=BioWink GmbH
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-06-10 13:39:49+00:00
Valid To: 3013-10-11 13:39:49+00:00
Issuer: O=BioWink GmbH
Serial Number: 0x53970aa5
Hash Algorithm: sha1
md5: 2a978bcc2b086ea97352b93b1ffaa195
sha1: 5d715c12cedec3a3dd04556188557ad9e5214f90
sha256: b19254e1edb19ffb52546ef5b4e11851430e95b042e06d4ad777ba69d672d8f6
sha512: 7590f99fe01fdf3a2c9e561dd1d3d3ffd705f31fb550ca99725979d368dd72c7c137dc70fee896520555debd58cc2ce61a249604f7dc17c12c12340ad70d696b
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: b3c8fd18cf314b86f31944756d5cc789a1965d7c6c2f17e703c023c676f95692
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

PERMISSION	STATUS	INFO	DESCRIPTION
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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.clue.android.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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.TAGS check
SIM operator check
network operator name check</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-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.helloclue.ui.MainActivity	Schemes: clue://, Hosts: premium-store, cycle, tracking, analysis, content, mode-selection, settings,

ACTIVITY	INTENT
net.openid.appauth.RedirectUriReceiverActivity	Schemes: fb456799567776359://, com.helloclue://, Paths: /authorize/,

NETWORK SECURITY

HIGH: 0 | WARNING: 0 | INFO: 0 | SECURE: 1

NO	SCOPE	SEVERITY	DESCRIPTION
1	helloclue.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: ++MBgDH5WGvL9Bcn5Be30cRcL0f5O+NyoXuWtQdX1aI= Digest: SHA-256,Pin: f0KW/FtqTjs108NpYj42SrGvOB2PpxIVM8nWxjPqJGE= Digest: SHA-256,Pin: NqvDJlas/GRcYbcWE8S/IceH9cq77kg0jVhZeAPXq8k= Digest: SHA-256,Pin: 9+ze1cZgR9KO1kZrVDxA4HQ6voHRCSVNz4RdTCx4U8U= Digest: SHA-256,Pin: KwccWaCgrnaw6tsrrSO61FgLacNgG2MMLq8GE6+oP5I= Digest: SHA-256]

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: **9** | 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	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Activity (net.openid.appauth.RedirectUriReceiverActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (com.helloclue.utils.test.TestActivity) 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	TaskAffinity is set for activity (com.braze.push.NotificationTrampolineActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
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	Activity (androidx.compose.ui.tooling.PreviewActivity) 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.
8	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [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.
9	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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.
10	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: 5 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A2/d.java A5/d.java A5/j.java A5/k.java A5/l.java A6/f.java A6/i.java B2/e.java B5/A.java B5/AbstractC0204e.java B5/C0206g.java B5/D.java B5/G.java B5/p.java B5/q.java B5/x.java B5/y.java C2/c.java C2/s.java Ci/F.java D2/g.java D2/n.java D2/o.java Db/a.java E0/B.java E0/t.java E5/b.java F/E0.java F5/b.java F5/d.java F6/b.java F6/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				F6/g.java Gc/c.java Gk/a.java H1/b.java H1/c.java H1/g.java Ik/b.java J1/d.java J5/f.java K0/a.java K6/a.java K6/e.java K6/h.java M/C0.java Pc/Y.java Pk/n.java Qk/d.java R0/c.java R3/b.java Rc/o.java T1/C0601o.java T1/G.java Ta/L.java Th/f.java Th/h.java U5/G0.java U5/M.java U5/c1.java U5/j1.java U5/n1.java V0/d.java V1/C.java V1/C0742c0.java V1/F.java V1/Z.java V1/p0.java Vh/c.java W6/c.java X5/a.java X6/b.java Xh/a.java Yi/a.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	Xi/c.java Xj/b.java Y/e.java Y6/c.java Y7/d.java Y7/r.java Yb/c.java Ye/c.java Yj/d.java Z/a.java Z0/e.java Zi/u.java a6/C0900b.java b1/AbstractC1255b.java b1/C1259f.java b1/C1261h.java b1/C1265l.java b2/C1270b.java b4/C1277c.java c6/b.java com/adjust/sdk/Logger.java com/braze/support/BrazeLogger.java com/braze/ui/inappmessage/a.java com/datadog/android/rum/DdRumContentProvider.java com/helloclue/ClueUpdateManager.java d2/AbstractC1745s.java d2/BinderC1742p.java d2/C1741o.java f1/AbstractC1971g.java h/AbstractActivityC2181g.java h/AbstractC2185k.java h/C2187m.java h/C2192r.java h/LayoutInflaterFactory2C2195u.java h1/AbstractC2203b.java h1/n.java hb/e.java i1/g.java i1/i.java i2/C2311e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				j/g.java j/h.java j1/AbstractC2351d.java j2/C2356a.java j3/AbstractC2358b.java k/MenuC2417l.java k/ViewOnKeyListenerC2411f.java kg/C2475b.java l/AbstractC2550g0.java l/C2530T.java l/C2537a.java l/C2558k0.java l/C2575t.java l/C2579v.java l/DialogInterfaceOnClickListenerC2523L.java l/I0.java l/O0.java l/e1.java l/f1.java l/u1.java m1/p.java mi/C2713g.java n6/d.java o6/AbstractC2857a.java p3/w0.java p3/x0.java p3/z0.java q/C3097f.java q5/c.java q5/i.java q6/g.java r1/C3251c.java r1/C3274u.java r1/M.java r1/Y.java r1/r0.java r1/s0.java r1/w0.java r4/Z.java r6/C3313e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ri/b.java s2/C3698h.java t2/r.java u1/b.java v1/C3704t.java v6/g.java v6/i.java w1/C3749b.java w6/k.java x5/C3864a.java x5/HandlerC3865b.java x5/d.java x5/f.java x5/g.java x5/h.java x5/i.java x5/j.java y5/AbstractBinderC3955j.java y5/AbstractC3949d.java y5/AbstractC3958m.java y5/C3950e.java y5/HandlerC3952g.java z1/e.java z6/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	F6/i.java K6/a.java L6/b.java Lk/l.java Qh/a.java U5/AbstractC0689r0.java U5/C0675k.java U5/H.java U5/j1.java U5/q1.java com/braze/ui/inappmessage/a.java i2/C2308b.java q5/c.java q5/h.java q5/i.java r5/k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	C2/d.java M/C0483h0.java Q2/a.java com/braze/Constants.java com/braze/enums/CardKey.java com/braze/models/inappmessage/InAppMessageHtml.java com/braze/models/outgoing/AttributionData.java com/braze/push/BrazeNotificationUtils.java com/braze/push/BrazePushReceiver.java com/braze/support/StringUtils.java com/braze/ui/contentcards/ContentCardsFragment.java com/braze/ui/inappmessage/listeners/DefaultInAppMessageWebViewClientListener.java com/helloclue/user/data/remote/model/request/UserSessionRequest.java r4/C3283B.java r4/C3296m.java r4/E.java r4/F.java r4/G.java r4/O.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	A2/f.java bo/app/SharedPreferencesC1356e.java bo/app/a0.java bo/app/c1.java bo/app/f6.java bo/app/h5.java bo/app/j0.java bo/app/j1.java bo/app/k0.java bo/app/l0.java bo/app/m.java bo/app/m4.java bo/app/n6.java bo/app/p1.java bo/app/q4.java bo/app/q6.java bo/app/t0.java bo/app/t3.java bo/app/w6.java bo/app/y0.java com/braze/configuration/RuntimeAppConfigurationProvider.java com/braze/managers/BrazeGeofenceManager.java
5	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	G6/a.java J5/i.java Si/a.java Si/b.java Ti/a.java U5/n1.java com/adjust/sdk/Util.java com/braze/support/IntentUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	Pk/e.java Pk/h.java Pk/m.java Pk/n.java Vh/d.java
7	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	U5/n1.java com/braze/support/StringUtils.java
8	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	v6/i.java z6/f.java
9	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	X6/b.java Y6/c.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	Aa/q.java P2/a.java Y7/q.java Zi/u.java com/adjust/sdk/ActivityHandler.java com/adjust/sdk/InstallReferrerHuawei.java com/adjust/sdk/a.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/support/UriUtils.java j7/g.java l/e1.java mi/C2713g.java o7/C2859b.java
00089	Connect to a URL and receive input stream from the server	command network	K6/a.java Y6/c.java bo/app/v0.java oi/C2879b.java
00030	Connect to the remote server through the given URL	network	U5/P.java bo/app/v0.java com/adjust/sdk/AdjustLinkResolution.java oi/C2879b.java
00109	Connect to a URL and get the response code	network command	D2/q.java K6/a.java U5/P.java Y6/c.java bo/app/v0.java oi/C2879b.java
00191	Get messages in the SMS inbox	sms	Y7/d.java com/adjust/sdk/a.java l/e1.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	A3/d.java Aa/q.java O3/f.java T1/G.java Ta/v.java U5/G0.java U5/RunnableC0703y0.java U5/n1.java Y7/d.java Y7/q.java Zi/u.java bd/C1311C.java com/adjust/sdk/ActivityHandler.java com/adjust/sdk/PreinstallUtil.java com/braze/Braze.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/inappmessage/views/InAppMessageHtmlBaseView.java com/braze/ui/support/UriUtils.java com/helloclue/pushnotification/ClueFirebaseMessagingService.java dg/C1784e.java lb/H.java mi/C2713g.java net/openid/appauth/AuthorizationManagementActivity.java o7/C2859b.java xe/C3880b.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	A3/d.java Y7/q.java Zi/u.java net/openid/appauth/AuthorizationManagementActivity.java o7/C2859b.java xe/C3880b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	I3/b.java K3/h.java Mi/j.java Sh/b.java Uk/v.java Xi/c.java b2/AbstractC1272d.java b2/C1270b.java b2/f.java bo/app/m0.java com/adjust/sdk/PreinstallUtil.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java i1/i.java j1/AbstractC2351d.java qi/C3166a.java
00078	Get the network operator name	collection telephony	Th/i.java bo/app/k0.java
00091	Retrieve data from broadcast	collection	C4/d.java U5/G0.java Xj/b.java Z/a.java com/braze/push/BrazeNotificationUtils.java com/helloclue/ui/MainActivity.java l3/n.java net/openid/appauth/AuthorizationManagementActivity.java w2/C3752c.java
00009	Put data in cursor to JSON object	file	C2/i.java H7/c.java hb/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00123	Save the response to JSON after connecting to the remote server	network command	bo/app/u1.java bo/app/v0.java
00108	Read the input stream from given URL	network command	U5/H0.java U5/O.java
00012	Read data and put it into a buffer stream	file	K3/h.java qi/C3166a.java
00187	Query a URI and check the result	collection sms calllog calendar	C2/s.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	C2/s.java
00022	Open a file from given absolute path of the file	file	A/Y.java Dk/g.java X2/d.java bd/C1311C.java bo/app/f6.java com/braze/Braze.java com/braze/images/DefaultBrazeImageLoader.java com/braze/support/BrazeFileUtils.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java
00162	Create InetSocketAddress object and connecting to it	socket	Pk/c.java Pk/n.java
00163	Create new Socket and connecting to it	socket	Pk/c.java Pk/n.java com/adjust/sdk/network/ActivityPackageSender.java

RULE ID	BEHAVIOUR	LABEL	FILES
00026	Method reflection	reflection	kj/z.java rj/C3358i.java
00024	Write file after Base64 decoding	reflection file	X2/d.java
00016	Get location info of the device and put it to JSON object	location collection	com/braze/models/outgoing/BrazeLocation.java
00014	Read file into a stream and put it into a JSON object	file	Sh/b.java
00096	Connect to a URL and set request method	command network	K6/a.java
00114	Create a secure socket connection to the proxy address	network command	Lk/k.java
00147	Get the time of current location	collection location	h/C2192r.java
00075	Get location of the device	collection location	h/C2192r.java
00115	Get last known location of the device	collection location	h/C2192r.java
00189	Get the content of a SMS message	sms	Rc/t.java
00188	Get the address of a SMS message	sms	Rc/t.java
00200	Query data from the contact list	collection contact	Rc/t.java
00201	Query data from the call log	collection calllog	Rc/t.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://clue-release.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/470118402803/namespaces/firebase:fetch?key=AIzaSyCyH_KVVXvycinhKwRLVnYA1JNnJv0YTW4 is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'latest_version': '0', 'min_supported_os_version': '0', 'min_supported_version_bubbles_mode': '0', 'min_supported_version_normal_mode': '0', 'unsupported_versions_bubbles_mode': '[]', 'unsupported_versions_normal_mode': '[]', 'update_url': 'market://details?id=com.clue.android'}, 'state': 'UPDATE', 'templateVersion': '39'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	4/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	4/44	com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_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
app.eu.adjust.com	ok	**IP:** 185.151.204.60 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
gdpr.adjust.world	ok	**IP:** 185.151.204.40 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.tiktok.com	ok	**IP:** 104.79.0.26 **Country:** United States of America **Region:** Michigan **City:** Saint Clair Shores **Latitude:** 42.496979 **Longitude:** -82.888809 **View:** Google Map
gdpr.tr.adjust.com	ok	**IP:** 195.244.54.7 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map
www.googleadservices.com	ok	**IP:** 74.125.21.155 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app.adjust.net.in	ok	**IP:** 185.151.204.32 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
clue-release.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
goo.gle	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
zendesk.helloclue.com	ok	**IP:** 54.76.71.139 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
app.adjust.com	ok	**IP:** 185.151.204.11 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sdk.iad-01.braze.com	ok	**IP:** 104.18.39.68 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
plus.google.com	ok	**IP:** 64.233.185.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
issuetracker.google.com	ok	**IP:** 64.233.177.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
gdpr.adjust.com	ok	**IP:** 185.151.204.51 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
oauth2.googleapis.com	ok	**IP:** 74.125.21.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
subscription.tr.adjust.com	ok	**IP:** 195.244.54.7 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map
helloclue.com	ok	**IP:** 18.238.109.70 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
subscription.adjust.world	ok	**IP:** 185.151.204.44 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
play.google.com	ok	**IP:** 172.253.124.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
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
github.com	ok	**IP:** 140.82.112.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebase.google.com	ok	**IP:** 74.125.136.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
twitter.com	ok	**IP:** 162.159.140.229 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
developer.android.com	ok	**IP:** 64.233.176.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 142.251.15.104 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.braze.com	ok	**IP:** 104.17.227.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
gdpr.eu.adjust.com	ok	**IP:** 185.151.204.60 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
subscription.eu.adjust.com	ok	**IP:** 185.151.204.60 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
gdpr.us.adjust.com	ok	**IP:** 185.151.204.70 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sondheim.braze.com	ok	**IP:** 172.64.144.252 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
app-measurement.com	ok	**IP:** 64.233.177.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app.usertesting.com	ok	**IP:** 151.101.130.49 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.helloclue.com	ok	**IP:** 18.155.173.109 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.instagram.com	ok	**IP:** 31.13.70.174 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
subscription.adjust.net.in	ok	**IP:** 185.151.204.34 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
biowink.zendesk.com	ok	**IP:** 216.198.54.6 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
graph.facebook.com	ok	**IP:** 31.13.70.1 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
app.adjust.world	ok	**IP:** 185.151.204.41 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
accounts.google.com	ok	**IP:** 172.217.215.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebaseinstallations.googleapis.com	ok	**IP:** 172.253.124.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
subscription.us.adjust.com	ok	**IP:** 185.151.204.70 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
support.helloclue.com	ok	**IP:** 216.198.53.6 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
app.tr.adjust.com	ok	**IP:** 195.244.54.7 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map
gdpr.adjust.net.in	ok	**IP:** 185.151.204.33 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
app.us.adjust.com	ok	**IP:** 185.151.204.70 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
dust.k8s.test-001.d-usw-2.braze.com	ok	No Geolocation information available.
images.ctfassets.net	ok	**IP:** 18.238.109.20 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
subscription.adjust.com	ok	**IP:** 185.151.204.52 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
google.com	ok	**IP:** 142.250.9.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xmlpull.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
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
goo.gl	ok	**IP:** 64.233.176.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	y5/BinderC3954i.java

EMAIL	FILE
johndoe@email.com	fd/C2030c.java
test@helloclue.com	ld/C2644c.java
trust@helloclue.com hello@helloclue.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Snowplow	Analytics	https://reports.exodus-privacy.eu.org/trackers/108

HARDCODED SECRETS

POSSIBLE SECRETS
"buyscreen_review_1_user" : "Quiggles07"
"buyscreen_review_2_user" : "Swebz89"

POSSIBLE SECRETS
"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"
"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"
"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"
"firebase_database_url" : "https://clue-release.firebaseio.com"
"google_api_key" : "AIzaSyCyH_KVVXvycinhKwRLVnYA1JNnJv0YTW4"
"google_crash_reporting_api_key" : "AIzaSyCyH_KVVXvycinhKwRLVnYA1JNnJv0YTW4"
"more_account_auth_type_connected" : "Connected"
59e48ee92b9443126493d934d92bcb4c
4552151eacfadc212d226d404953a57c
0d1d9178958646156132951c8b7dbcb5
c5e3b1e194bc11a6915d82baa0129a15
b9b1959d7dd42a631bcee90e86d93c537
8ab20d23-3899-4aa7-a175-651e0278cf60
70c940fedb2f593c8f902af00648bafa
0fad9940-b757-4760-aa4a-4376e3ef1528

POSSIBLE SECRETS
37a6259cc0c1dae299a7866489dff0bd
30820268308201d102044a9c4610300d06092a864886f70d0101040500307a310b3009060355040613025553310b3009060355040813024341311230100603550407130950616c6f20416c746f3118301606035504a130f46616365626f6f6b204d6f62696c653111300f060355040b130846616365626f6f6b311d301b0603550403131446616365626f6f6b20436f72706f726174696f6e3020170d3039303833313231353231365a180f32303530303932353231353231365a307a310b3009060355040613025553310b3009060355040813024341311230100603550407130950616c6f20416c746f3118301606035504a130f46616365626f6f6b204d6f62696c653111300f060355040b130846616365626f6f6b311d301b0603550403131446616365626f6f6b20436f72706f726174696f6e30819f300d06092a864886f70d010101050003818d0030818902818100c207d51df8eb8c97d93ba0c8c1002c928fab00dc1b42fca5e66e99cc3023ed2d214d822bc59e8e35ddcf5f44c7ae8ade50d7e0c434f500e6c131f4a2834f987fc46406115de2018ebbb0d5a3c261bd97581ccfef76afc7135a6d59e8855ecd7eacc8f8737e794c60a761c536b72b11fac8e603f5da1a2d54aa103b8a13c0dbc10203010001300d06092a864886f70d0101040500038181005ee9be8bcbb250648d3b741290a82a1c9dc2e76a0af2f2228f1d9f9c4007529c446a70175c5a900d5141812866db46be6559e2141616483998211f4a673149fb2232a10d247663b26a9031e15f84bc1c74d141ff98a02d76f85b2c8ab2571b6469b232d8e768a7f7ca04f7abe4a775615916c07940656b58717457b42bd928a2
9b6ddd180e63aca538398db4d3f34c87
51513f833c66f856ae497d6b3fc4c148
7620d2f70890151a7dd49807de935b19
357fc505794e7da099a1861cf802290b
a36b4ba9bb0247f28bc5be6e0f06711f
2d98be7493ef375453e9188af14eeeea
8ae6f9f021316b8ae0671e3cc95ac618
3071c8717539de5d5353f4c8cd59a032
7d73d21f1bd82c9e5268b6dcf9fde2cb
7c656a874acbd37c6dc6538162d74eef

POSSIBLE SECRETS
c1a00b1edb673b95984cf834980617cc
5c68328d95b139c12fb0b7ef5f31cd29
9b3388437f5e687486a720abfbee0e70
b4c559f1d1c1f9ceb37a33e318a7feed

PLAYSTORE INFORMATION

Title: Clue Cycle & Period Tracker

Score: 4.4181914 **Installs:** 50,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.clue.android

Developer Details: Clue Period Tracker by BioWink, Clue+Period+Tracker+by+BioWink, None, http://helloclue.com, support@helloclue.com,

Release Date: Oct 9, 2014 **Privacy Policy:** Privacy link

Description:

Clue Period & Ovulation Tracker is a science-packed health and period tracker designed to decode your menstrual cycle in every life stage – from your first period to hormonal changes, conception, pregnancy, and even perimenopause. Clue's period tracker helps you understand your body's unique rhythm, offering deep insights into your menstrual cycle, mental health, PMS, and fertility with advanced ovulation predictions and birth control tracking. Your health data is protected with Clue under the world's strictest data privacy standards (the EU GDPR), so you always stay in control. □□□ Period Tracker for Menstrual Cycle Tracking • Clue's smart algorithm powers a reliable period tracker with accurate predictions for your period, PMS, ovulation, and more. • Plan your life better with Clue's period calendar, ovulation calculator, and fertility tools. • Use Clue as your daily period tracker to monitor 200+ factors like mood, energy, sleep, and mental health—and how they relate to your menstrual cycle. • Clue can help as a period tracker for teens or anyone with irregular cycles, helping identify patterns and manage symptoms like PMS, cramps, PCOS, or endometriosis. Ovulation Calculator & Fertility Tracker • Use Clue as both an ovulation calculator and a fertility tracker—no need for ovulation strips or temperature tracking. • Clue Conceive's clinically-tested algorithm delivers daily fertility insights, ovulation tracking, and ovulation estimates—helping you get pregnant faster. • Pinpoint ovulation with options like basal body temperature tracking (BBT), all within your period tracker app. Pregnancy Tracker & Weekly Support • Track your pregnancy week-by-week using Clue's pregnancy tracker with guidance from certified Nurse Midwives. • Stay on top of pregnancy symptoms and milestones using Clue as both a pregnancy tracker and comprehensive period tracker before, during, and after pregnancy. Period Tracker Reminders & Birth Control Alerts • Set helpful reminders in your period tracker for birth control, PMS, ovulation, and your next period. • Get alerts from your period tracker when your cycle changes or PMS symptoms shift. Track Health Conditions and Irregular Cycles • Clue is a reliable period tracker for people with PCOS, endometriosis, irregular periods, or perimenopause. • Understand your menstrual health better

with tools for period tracking, symptom tracking, and cycle syncing. • Use Clue as your go-to irregular period tracker for cycles that aren't consistent. Additional Cycle Tracking Features in Clue: • Explore over 300 expert-written articles on menstruation, fertility, pregnancy, and more—all accessible within your period tracker. • Personalize with daily notes and custom tracking tags. • Use Clue Connect to share your cycle insights with partners and stay aligned on your PMS, period, and fertile days. Clue's award-winning period tracker is backed by science, with partnerships involving researchers at UC Berkeley, Harvard, and MIT. Be part of a global movement advancing menstrual health knowledge for everyone with a cycle. Note: Clue Period Tracker and Ovulation Tracker should not be used as a form of contraception. Visit support.helloclue.com for help and resources. Download Clue to start using your free period tracker today. Subscribe for deeper insights and unlock premium features in your ovulation tracker, pregnancy tracker, and perimenopause tools.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 21:11:22	Generating Hashes	OK
2025-08-29 21:11:22	Extracting APK	OK
2025-08-29 21:11:22	Unzipping	OK
2025-08-29 21:11:22	Parsing APK with androguard	OK
2025-08-29 21:11:22	Extracting APK features using aapt/aapt2	OK
2025-08-29 21:11:22	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 21:11:24	Parsing AndroidManifest.xml	OK

2025-08-29 21:11:24	Extracting Manifest Data	OK
2025-08-29 21:11:24	Manifest Analysis Started	OK
2025-08-29 21:11:24	Reading Network Security config from network_security_config.xml	OK
2025-08-29 21:11:24	Parsing Network Security config	OK
2025-08-29 21:11:24	Performing Static Analysis on: Clue (com.clue.android)	OK
2025-08-29 21:11:25	Fetching Details from Play Store: com.clue.android	OK
2025-08-29 21:11:26	Checking for Malware Permissions	OK
2025-08-29 21:11:26	Fetching icon path	OK
2025-08-29 21:11:26	Library Binary Analysis Started	OK
2025-08-29 21:11:26	Reading Code Signing Certificate	OK
2025-08-29 21:11:26	Running APKiD 2.1.5	OK

2025-08-29 21:11:29	Detecting Trackers	OK
2025-08-29 21:11:30	Decompiling APK to Java with JADX	OK
2025-08-29 21:11:44	Converting DEX to Smali	OK
2025-08-29 21:11:44	Code Analysis Started on - java_source	OK
2025-08-29 21:11:48	Android SBOM Analysis Completed	OK
2025-08-29 21:12:00	Android SAST Completed	OK
2025-08-29 21:12:00	Android API Analysis Started	OK
2025-08-29 21:12:12	Android API Analysis Completed	OK
2025-08-29 21:12:12	Android Permission Mapping Started	OK
2025-08-29 21:12:22	Android Permission Mapping Completed	OK
2025-08-29 21:12:22	Android Behaviour Analysis Started	OK

2025-08-29 21:12:36	Android Behaviour Analysis Completed	OK
2025-08-29 21:12:36	Extracting Emails and URLs from Source Code	OK
2025-08-29 21:12:41	Email and URL Extraction Completed	OK
2025-08-29 21:12:41	Extracting String data from APK	OK
2025-08-29 21:12:42	Extracting String data from Code	OK
2025-08-29 21:12:42	Extracting String values and entropies from Code	OK
2025-08-29 21:12:44	Performing Malware check on extracted domains	OK
2025-08-29 21:12:47	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.