ANDROID STATIC ANALYSIS REPORT

Guardian (11.6.2)

File Name:	com.glic.group.ga.mobile_116201.apk
Package Name:	com.glic.group.ga.mobile
Scan Date:	Aug. 29, 2025, 11:02 p.m.
App Security Score:	47/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	10	8	1	2

FILE INFORMATION

File Name: com.glic.group.ga.mobile_116201.apk
Size: 35.53MB
MD5: 73d2a59ac1d52e096dc52ac48834bfe1
SHA1: ef14532e2ab0ebe846d0e58e1cd396bed9bdd4da
SHA256: 1a298180ff1599582c078102c3dd5ed7c4b013c5dc6ff23ac0a55705eb36936d

APP INFORMATION

App Name: Guardian
Package Name: com.glic.group.ga.mobile
Main Activity: com.glic.group.ga.mobile.Activity.MainActivity
Target SDK: 34
Min SDK: 31
Max SDK:
Android Version Name: 11.6.2

Android Version Code: 116201

APP COMPONENTS

Activities: 14
Services: 7
Receivers: 4
Providers: 3
Exported Activities: 0
Exported Services: 0
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: None
X.509 Subject: C=US, ST=NY, L=New York, O=Guardian Life, OU=Guardian Life, CN=Guardian Life
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-06-06 15:28:31+00:00
Valid To: 2037-05-31 15:28:31+00:00
Issuer: C=US, ST=NY, L=New York, O=Guardian Life, OU=Guardian Life, CN=Guardian Life
Serial Number: 0x4fcf771f
Hash Algorithm: sha1
md5: 993046ada57b6e36dc6af758e0ed5bcc
sha1: 64b4b5005df222a0d5836fd2decf44ab1428a131
sha256: ef6ea35041999e1b0257a9bf92ae148c02d6f554b2486443f1fe52896d6b44cc
sha512: 2f36d35feb686b3cc0697dcc4ef4bf62da2147bdcd92a4b32a84ae9aaed7041736ef40ae8f3275cb640e8c41cfe2ab0757e39be20fecd2cb618546dc50fdcd2f
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: f96a5208e30fa0f58f96143384967b46c764aa414edea598f383773b7d24957c
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_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.glic.group.ga.mobile.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>73d2a59ac1d52e096dc52ac48834bfe1.apk</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>possible VM check</td></tr></table></td></tr>
<tr><td>classes.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table></td></tr>
<tr><td>classes2.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.TAGS check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table></td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
network operator name check
possible VM check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	warning	Base config is configured to trust system certificates.
2	*	info	Base config is configured to trustbundled certs @raw/sectigo_rsa_extended_validation_secure_server_ca.
3	*	info	Base config is configured to trustbundled certs @raw/sectigo_rsa_organization_validation_secure_server_ca.

NO	SCOPE	SEVERITY	DESCRIPTION
4	*	info	Base config is configured to trustbundled certs @raw/usertrust_rsa_certification_authority.
5	group.api.guardianlife.com	info	Certificate pinning expires on 2030-12-30. After this date pinning will be disabled. [Pin: hEJ5FNYP7ZpNILySZtJgiP6UtW3ClYUTRFxXGqWSWQ0= Digest: SHA-256]
6	apisvc.guardianlife.com	info	Certificate pinning expires on 2030-12-30. After this date pinning will be disabled. [Pin: hEJ5FNYP7ZpNILySZtJgiP6UtW3ClYUTRFxXGqWSWQ0= Digest: SHA-256]
7	guardiananytime.com	info	Certificate pinning expires on 2030-12-30. After this date pinning will be disabled. [Pin: hEJ5FNYP7ZpNILySZtJgiP6UtW3ClYUTRFxXGqWSWQ0= 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: **1** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

HIGH: **1** | WARNING: **5** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				B2/a.java C1/c.java C2/A.java C2/C.java C2/C0734c.java C2/d.java C2/l.java C2/n.java C2/o.java C2/s.java D0/N.java F1/a.java G2/a.java G2/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				G2/j.java I/u0.java I2/f.java I2/q.java I2/r.java I2/t.java I2/u.java I2/v.java J2/d.java L1/C0993a.java L1/n.java L2/d.java L2/l.java N2/b.java P1/a.java P2/a.java Q0/L.java Q2/b.java Q2/h.java Q2/k.java R0/a.java T1/n.java Y1/a.java a1/C1431d.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/c.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java com/bumptech/glide/request/j.java com/glic/group/ga/mobile/application/BaseApplication.java com/glic/member/client/authLibrary/OktaIdentityProvider$logout$1.java com/glic/member/client/authLibrary/OktaIdentityProvider.java com/qualtrics/digital/ActionSet.java com/qualtrics/digital/DateExpression.java com/qualtrics/digital/DayExpression.java com/qualtrics/digital/DurationExpression.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	com/qualtrics/digital/EmbeddedFeedbackOrchestrator.java com/qualtrics/digital/InterceptDefinition.java com/qualtrics/digital/Properties.java com/qualtrics/digital/Qualtrics.java com/qualtrics/digital/QualtricsLog.java com/qualtrics/digital/QualtricsPopOverFragment.java com/qualtrics/digital/QualtricsSurveyActivity.java com/qualtrics/digital/QualtricsSurveyExpression.java com/qualtrics/digital/ServiceInterceptor.java com/qualtrics/digital/TimeExpression.java com/qualtrics/digital/VariableExpression.java com/qualtrics/digital/ViewCountExpression.java com/qualtrics/digital/WebViewInterface.java com/qualtrics/digital/resolvers/CustomPropertyResolver.java com/qualtrics/digital/resolvers/DateTimeTypeResolvers.java com/qualtrics/digital/resolvers/QualtricsSurveyResolver.java com/qualtrics/digital/resolvers/SamplingResolver.java com/qualtrics/digital/resolvers/TimeSpentInAppResolver.java com/qualtrics/digital/resolvers/ViewCountResolver.java d1/f.java e/AbstractC2077e.java es/voghdev/pdfviewpager/library/subscaleview/SubsamplingScaleImageView.java es/voghdev/pdfviewpager/library/subscaleview/decoder/SkiaPooledImageRegionDecoder.java h0/C2188f.java k1/AbstractC2259d.java m1/C2364h.java n/d.java n/e.java n/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				n/h.java n/i.java n/k.java n/l.java r2/C2640a.java s2/d.java s2/e.java s3/AbstractC2745a.java u2/C2909c.java u2/C2911e.java v2/h.java v2/i.java v2/k.java v2/q.java v2/z.java w2/i.java w2/j.java x2/C3115e.java x2/i.java y2/ExecutorServiceC3196a.java z2/C3234c.java z2/d.java z2/f.java z2/r.java z2/s.java
				K3/Authenticator.java K3/FormValue.java K3/Message.java M/J.java P0/C1085g.java P0/P.java R/C1196b0.java X5/C1330h0.java com/glic/group/ga/mobile/Activity/LocationChangeActivity.java com/glic/group/ga/mobile/BuildConfig.java com/glic/group/ga/mobile/application/BaseApplication.java com/glic/group/ga/mobile/controller/DentistSearchActivityManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/glic/group/ga/mobile/group/presentation/claims/data/model/response/LetterSearchResponse.java com/glic/group/ga/mobile/group/presentation/finddentist/viewmodel/DentistViewModel.java com/glic/member/client/authLibrary/ApigeeOAuthGenerateResponse.java com/glic/member/client/authLibrary/OktaEvent.java com/qualtrics/digital/EmbeddedFeedbackUtils.java com/qualtrics/digital/EmbeddedFeedbackUtilsJava.java com/qualtrics/digital/ExpressionDeserializer.java com/qualtrics/digital/QualtricsPopOverFragment.java com/qualtrics/digital/SDKUtils.java com/qualtrics/digital/XMDUtils.java com/qualtrics/digital/utils/TranslationUtils.java k2/InterfaceC2266c.java k3/C2272c.java t2/h.java v2/d.java v2/p.java v2/x.java
3	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/glic/group/ga/mobile/idcard/LoginActivity.java
4	Calling Cipher.getInstance("AES") will return AES ECB mode by default. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	com/glic/group/ga/mobile/common/AESEncryption.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	com/glic/group/ga/mobile/common/AESEncryption.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/qualtrics/digital/SamplingUtil.java q4/AbstractC2599a.java q4/C2600b.java r4/C2643a.java
7	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/glic/group/ga/mobile/helpers/KeyStoreManager.java
8	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/qualtrics/digital/QualtricsSurveyFragment.java
9	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	r3/C2641a.java v3/C2944a.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/bumptech/glide/load/a.java com/glic/group/ga/mobile/helpers/DocPrintManager.java okio/x.java r2/C2640a.java u1/m.java z2/f.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	L1/C0993a.java L1/n.java com/glic/group/ga/mobile/Activity/ActivityUtilsKt.java com/glic/group/ga/mobile/Activity/MainActivity.java com/glic/group/ga/mobile/RateThisApp.java com/glic/group/ga/mobile/group/presentation/finddentist/OfficeDetailKt.java com/glic/group/ga/mobile/group/presentation/finddentist/screens/location_instructions/LocationInstructionsSheetKt.java com/glic/group/ga/mobile/group/utils/FapUtilsKt.java com/glic/group/ga/mobile/helpers/ClickableURLSpan.java com/glic/group/ga/mobile/idcard/LoginActivity.java com/glic/group/ga/mobile/idcard/ProfileActivity.java com/qualtrics/digital/QualtricsNotificationManager.java com/qualtrics/digital/QualtricsPopOverActivity.java com/qualtrics/digital/QualtricsSurveyFragment.java
00091	Retrieve data from broadcast	collection	com/qualtrics/digital/QualtricsNotificationManager.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	L1/C0993a.java com/glic/group/ga/mobile/group/utils/FapUtilsKt.java com/qualtrics/digital/QualtricsNotificationManager.java

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/glic/group/ga/mobile/group/utils/FileUtils.java u2/C2909c.java
00202	Make a phone call	control	com/glic/group/ga/mobile/group/utils/FapUtilsKt.java
00203	Put a phone number into an intent	control	com/glic/group/ga/mobile/group/utils/FapUtilsKt.java
00036	Get resource file from res/raw directory	reflection	com/glic/group/ga/mobile/Activity/MainActivity.java com/glic/group/ga/mobile/RateThisApp.java com/glic/group/ga/mobile/group/utils/FapUtilsKt.java com/glic/group/ga/mobile/helpers/ClickableURLSpan.java es/voghdev/pdfviewpager/library/subscaleview/SubsamplingScaleImageView.java j2/e.java
00022	Open a file from given absolute path of the file	file	com/glic/group/ga/mobile/Activity/IDCardViewerActivity.java f2/InterfaceC2119a.java u1/m.java v3/AbstractC2945b.java
00026	Method reflection	reflection	l4/C0864a.java l4/C0865b.java
00024	Write file after Base64 decoding	reflection file	com/glic/group/ga/mobile/idcard/IDCardListFragment.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/j.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/j.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/j.java

RULE ID	BEHAVIOUR	LABEL	FILES
00078	Get the network operator name	collection telephony	s3/AbstractC2747c.java
00132	Query The ISO country code	telephony collection	s3/AbstractC2747c.java
00121	Create a directory	file command	com/glic/group/ga/mobile/idcard/IDCardViewActivity.java
00125	Check if the given file path exist	file	com/glic/group/ga/mobile/idcard/IDCardViewActivity.java
00161	Perform accessibility service action on accessibility node info	accessibility service	m1/C2364h.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	m1/C2364h.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/846825620717/namespaces/firebase:fetch?key=AIzaSyCUGl0Lt-T17D5azTTqQgj_TiOazZSuDVI is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'AppMinVersion': '11.1.0', 'ForceUpdate': 'true', 'HideAbsenceCommunicationDelete': 'false', 'Maintenance': 'false', 'MaintenanceMessage': "We'll be back. We're busy updating the app. We'll be back as soon as possible.", 'OktaAuthentication': 'true', 'OktaBaseURL': 'https://signin.guardianlife.com/signin/', 'ProfileV2Enabled': 'true', 'UpdateAvailable': 'true'}, 'state': 'UPDATE', 'templateVersion': '37'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.WAKE_LOCK, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	2/44	com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID

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
maps.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
group.api.guardianlife.com	ok	**IP:** 45.60.150.30 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
www.guardiananytime.com	ok	**IP:** 45.60.11.160 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
mobile.events.data.microsoft.com	ok	**IP:** 20.189.173.9 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
issuetracker.google.com	ok	**IP:** 64.233.177.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.manageddentalcare.net	ok	**IP:** 45.223.97.187 **Country:** United States of America **Region:** California **City:** Redwood City **Latitude:** 37.532440 **Longitude:** -122.248833 **View:** Google Map
survey.qualtrics.com	ok	**IP:** 23.38.162.28 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
login.guardianlife.com	ok	**IP:** 3.15.167.137 **Country:** United States of America **Region:** Ohio **City:** Columbus **Latitude:** 39.961182 **Longitude:** -82.998787 **View:** Google Map
www.avesis.com	ok	**IP:** 141.193.213.11 **Country:** United States of America **Region:** Texas **City:** Austin **Latitude:** 30.271158 **Longitude:** -97.741699 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
apisvc.guardianlife.com	ok	**IP:** 45.60.11.160 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
client.libertydentalplan.com	ok	**IP:** 52.175.202.25 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
teledentix.com	ok	**IP:** 20.228.82.3 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.guardianlife.com	ok	**IP:** 45.60.11.160 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.dominiondentists.com	ok	**IP:** 8.43.31.32 **Country:** United States of America **Region:** Pennsylvania **City:** Philadelphia **Latitude:** 39.952339 **Longitude:** -75.163788 **View:** Google Map
microsite.versanthealth.com	ok	**IP:** 104.18.30.10 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.vsp.com	ok	**IP:** 18.238.96.8 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
maps.google.com	ok	**IP:** 173.194.219.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
in.appcenter.ms	ok	**IP:** 20.57.103.21 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map
s-s.s	ok	No Geolocation information available.
signin.guardianlife.com	ok	**IP:** 45.60.11.160 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
idoc.davisvision.com	ok	**IP:** 134.195.63.15 **Country:** United States of America **Region:** Texas **City:** San Antonio **Latitude:** 29.425426 **Longitude:** -98.489349 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
s.qualtrics.com	ok	**IP:** 23.38.162.28 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map

EMAILS

EMAIL	FILE
random@email.com	com/glic/group/ga/mobile/mfa/ComposableSingletons$MFAActivityKt$lambda6$1.java

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Microsoft Visual Studio App Center Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/243
Qualtrics		https://reports.exodus-privacy.eu.org/trackers/306

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "aab560160cd3434791a3500972766ab3"
"google_api_key" : "AIzaSyCUGl0Lt-T17D5azTTqQgj_TiOazZSuDVI"
"google_crash_reporting_api_key" : "AIzaSyCUGl0Lt-T17D5azTTqQgj_TiOazZSuDVI"
"password" : "Password"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
23456789abcdefghjkmnpqrstvwxyz
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

POSSIBLE SECRETS
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
733f8a2e-0352-4025-9d8b-30be58fd08f3
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
115792089210356248762697446949407573530086143415290314195533631308867097853951
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: Guardian® Dental & Vision

Score: 2.33 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.glic.group.ga.mobile

Developer Details: The Guardian Life Insurance Company of America, 5653449626263155179, None, https://www.guardianlife.com/, cru@glic.com,

Release Date: Jul 18, 2012 **Privacy Policy:** Privacy link

Description:

Easily access your Guardian Dental and Vision benefit information. - Find a Provider: Search for participating dental or vision providers by name or location - ID cards: View, download/add to Apple wallet or email your Dental and Vision ID cards. Use when making an appointment or at your next visit. - NEW View Dental benefit plan information - NEW View Dental claims status and history

SCAN LOGS

Timestamp	Event	Error
2025-08-29 23:02:06	Generating Hashes	OK
2025-08-29 23:02:06	Extracting APK	OK
2025-08-29 23:02:06	Unzipping	OK
2025-08-29 23:02:06	Parsing APK with androguard	OK
2025-08-29 23:02:06	Extracting APK features using aapt/aapt2	OK
2025-08-29 23:02:06	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 23:02:08	Parsing AndroidManifest.xml	OK

2025-08-29 23:02:08	Extracting Manifest Data	OK
2025-08-29 23:02:08	Manifest Analysis Started	OK
2025-08-29 23:02:08	Reading Network Security config from network_security_config.xml	OK
2025-08-29 23:02:08	Parsing Network Security config	OK
2025-08-29 23:02:08	Performing Static Analysis on: Guardian (com.glic.group.ga.mobile)	OK
2025-08-29 23:02:09	Fetching Details from Play Store: com.glic.group.ga.mobile	OK
2025-08-29 23:02:09	Checking for Malware Permissions	OK
2025-08-29 23:02:09	Fetching icon path	OK
2025-08-29 23:02:09	Library Binary Analysis Started	OK
2025-08-29 23:02:09	Reading Code Signing Certificate	OK

2025-08-29 23:02:10	Failed to get signature versions with apksigner	CalledProcessError(1, ['/jdk-22.0.2/bin/java', '-Xmx1024M', '-Djava.library.path=', '-jar', '/home/mobsf/Mobile-Security-Framework-MobSF/mobsf/StaticAnalyzer/tools/apksigner.jar', 'verify', '--verbose', '/home/mobsf/.MobSF/uploads/73d2a59ac1d52e096dc52ac48834bfe1/73d2a59ac1d52e096dc52ac48834bfe1.apk'])
2025-08-29 23:02:10	Running APKiD 2.1.5	OK
2025-08-29 23:02:12	Detecting Trackers	OK
2025-08-29 23:02:15	Decompiling APK to Java with JADX	OK
2025-08-29 23:02:32	Converting DEX to Smali	OK
2025-08-29 23:02:32	Code Analysis Started on - java_source	OK
2025-08-29 23:02:36	Android SBOM Analysis Completed	OK
2025-08-29 23:02:44	Android SAST Completed	OK
2025-08-29 23:02:44	Android API Analysis Started	OK
2025-08-29 23:02:52	Android API Analysis Completed	OK

2025-08-29 23:02:52	Android Permission Mapping Started	OK
2025-08-29 23:03:02	Android Permission Mapping Completed	OK
2025-08-29 23:03:03	Android Behaviour Analysis Started	OK
2025-08-29 23:03:14	Android Behaviour Analysis Completed	OK
2025-08-29 23:03:14	Extracting Emails and URLs from Source Code	OK
2025-08-29 23:03:32	Email and URL Extraction Completed	OK
2025-08-29 23:03:32	Extracting String data from APK	OK
2025-08-29 23:03:32	Extracting String data from Code	OK
2025-08-29 23:03:32	Extracting String values and entropies from Code	OK
2025-08-29 23:03:48	Performing Malware check on extracted domains	OK
2025-08-29 23:03:53	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.