ANDROID STATIC ANALYSIS REPORT

1

Accredo (2.34.0)

File Name:	com.accredohealth.accredo_28138.apk
Package Name:	com.accredohealth.accredo
Scan Date:	Aug. 29, 2025, 6:56 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	14	3	3	1

FILE INFORMATION

File Name: com.accredohealth.accredo_28138.apk
Size: 15.02MB
MD5: 3c30992f61d39cf06de747385b6a5299
SHA1: d5c332324b2b3b3789a9eb815ada610b45393151
SHA256: c64f4fe7a376df8196ce9b103363bd53fb87800bb21c47af859a5863bcb36951

APP INFORMATION

App Name: Accredo
Package Name: com.accredohealth.accredo
Main Activity: com.accredohealth.accredo.ui.AppMainActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 2.34.0

Android Version Code: 28138

APP COMPONENTS

Activities: 8
Services: 5
Receivers: 7
Providers: 3
Exported Activities: 2
Exported Services: 0
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: False
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: 2017-09-13 16:47:03+00:00
Valid To: 2047-09-13 16:47:03+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xb7f2b60ab4f9810661e2f5666da6ea5f02b6a197
Hash Algorithm: sha256
md5: b400ef07db4f78126630bce1118a9b9e
sha1: 260600f36a387f1b0f9e9e1c14a33a78ec3fb101
sha256: ffe6a4b6618f3070f6e561a257b8c6794360e703462784fa2e2039b591be712d
sha512: e48e508683161a4400e5a38820df0177d314cb350bab851a7e7b1d89ef869588816433c85b180977cc0aa4c4683604b9d557c368d45da5eeb90e74bc18c37cbd
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: e793942aaff7b45a6e0d9c94717ae85aecd39e074342c5dcbde5a47e0db0842e
Found 1 unique certificates
```

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
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_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.accredohealth.accredo.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

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>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.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>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.accredohealth.accredo.ui.ClearStackActivity	Schemes: accredo://, https://, Hosts: accredo.app.link, uutb.app.link,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

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

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/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	App Link assetlinks.json file not found [android:name=com.accredohealth.accredo.ui.ClearStackActivity] [android:host=https://accredo.app.link]	high	App Link asset verification URL (https://accredo.app.link/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 200). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
4	Activity (com.accredohealth.accredo.ui.ClearStackActivity) 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	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.
6	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.

NO	ISSUE	SEVERITY	DESCRIPTION
7	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: **7** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/apiguard3/internal/ce.java com/apiguard3/internal/setImportantForAutofill.java d8/a.java sh/a.java sh/b.java th/a.java x8/a.java x8/b.java zi/b.java
				a3/d.java a4/c.java ad/c.java be/a.java be/b.java be/c.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	c2/n0.java cc/a0.java cc/b.java cc/c.java cc/d0.java cc/e0.java cc/k.java cc/x.java cc/y.java com/launchdarkly/sdk/android/n0.java d3/f.java dc/d.java dc/i.java dc/j.java dc/n.java dc/u.java dc/y.java e1/f.java f/d.java f9/e.java fc/v.java gc/a.java gc/b0.java gc/b1.java gc/c.java gc/f1.java gc/o0.java gc/r0.java gc/s0.java gc/t0.java gc/v0.java gc/y.java ge/e.java gg/d0.java h0/t1.java i4/a.java i4/c.java j4/a.java j4/j.java jc/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				je/f.java je/h.java k3/d.java k8/a.java kc/e.java kc/l.java ld/a.java m/c.java mg/g.java mg/i.java n3/n.java nd/d.java ob/k.java oc/b.java p/d.java p/e.java p/f.java p/h.java p/i.java p/k.java p/l.java p2/l0.java q0/b.java q2/a.java q3/c.java q4/b.java qd/g.java rb/a.java t3/c.java uc/a.java uzhuaxzc/C0641m.java v2/c.java vd/i.java wc/a.java we/b.java x3/a.java xc/a.java xe/c.java y7/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	r7/d.java t7/k.java vb/m0.java vb/t0.java y8/c.java y8/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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/accredohealth/accredo/data/local/auth/Authentication.java com/accredohealth/accredo/data/local/copayassistance/AddCopayAssistanceCardCacheData.java com/accredohealth/accredo/data/local/copayassistance/EditCopayAssistanceCardCacheData.java com/accredohealth/accredo/data/local/patient/UserTokenAttribute.java com/accredohealth/accredo/data/local/payment/AddPaymentMethodCacheData.java com/accredohealth/accredo/data/remote/auth/AuthClient.java com/accredohealth/accredo/data/remote/auth/DeleteAccountRequest.java com/accredohealth/accredo/data/remote/interceptors/AuthHeaderInterceptor.java com/accredohealth/accredo/data/remote/patient/PatientUserTokenAttributeEntity.java com/accredohealth/accredo/data/remote/reminder/ReminderClient.java com/launchdarkly/sdk/LDContext.java eg/b.java eg/h.java eg/o.java l0/t0.java ni/f1.java o2/b0.java o7/a.java q0/a3.java q0/t1.java w7/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	i4/c.java we/c.java
6	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	j5/a0.java p/i.java
7	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	we/b.java
8	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	q8/w.java vd/w.java
9	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/apiguard3/internal/setAccessibilityDelegate.java
10	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	jf/o.java s8/b.java
11	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/adobe/marketing/mobile/assurance/internal/f0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	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	e6/q.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/apiguard3/internal/setAutofillId.java com/launchdarkly/sdk/android/l0.java gg/d0.java i4/c.java ib/d.java io/realm/internal/OsRealmConfig.java io/realm/internal/OsSharedRealm.java io/realm/q0.java t7/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	a8/b.java com/apiguard3/internal/setAccessibilityDelegate.java jb/i.java lh/m.java okio/Okio__JvmOkioKt.java t7/f.java v7/d.java we/c.java x3/a.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	a5/c.java a5/f.java com/accredohealth/accredo/ui/custom/j0.java com/adobe/marketing/mobile/assurance/internal/AssuranceExtension.java dc/e.java g8/b.java h5/h.java j4/a.java j4/j.java mg/c.java pg/a.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	dc/e.java g8/b.java j4/a.java mg/c.java
00036	Get resource file from res/raw directory	reflection	dc/e.java mg/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/accredohealth/accredo/notification/NotificationActionReceiver.java com/accredohealth/accredo/notification/ReminderNotificationReceiver.java mg/c.java
00014	Read file into a stream and put it into a JSON object	file	we/c.java
00078	Get the network operator name	collection telephony	com/adobe/marketing/mobile/assurance/internal/c.java e9/a.java mg/f0.java y7/i.java
00163	Create new Socket and connecting to it	socket	y7/q.java
00012	Read data and put it into a buffer stream	file	com/apiguard3/internal/setAccessibilityDelegate.java x3/a.java
00112	Get the date of the calendar event	collection calendar	c5/p.java gb/h.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	gg/o.java
00094	Connect to a URL and read data from it	command network	com/apiguard3/internal/setAccessibilityDelegate.java
00191	Get messages in the SMS inbox	sms	jg/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00003	Put the compressed bitmap data into JSON object	camera	ng/b.java
00161	Perform accessibility service action on accessibility node info	accessibility service	n3/n.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	n3/n.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://accredo-50845.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/182161255291/namespaces/firebase:fetch?key=AIzaSyDAyd_JjcKLEJr7YktEWWSFFGCjxXnRQAY. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	4/25	android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK
Other Common Permissions	2/44	com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
issuetracker.google.com	ok	**IP:** 64.233.177.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www-qa.accredo.acdo	ok	No Geolocation information available.
blobs.griffon.adobe.com	ok	No Geolocation information available.
device.griffon.adobe.com	ok	**IP:** 13.224.53.13 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
patient.accredo.com	ok	**IP:** 167.211.52.120 **Country:** United States of America **Region:** New Jersey **City:** Franklin Lakes **Latitude:** 41.009102 **Longitude:** -74.208122 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
wwwapps.ups.com	ok	**IP:** 23.222.206.62 **Country:** United States of America **Region:** Minnesota **City:** Minneapolis **Latitude:** 44.979969 **Longitude:** -93.263840 **View:** Google Map
bf08379irm.bf.dynatrace.com	ok	**IP:** 52.54.149.232 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www-uat.accredo.com	ok	**IP:** 167.18.110.116 **Country:** United States of America **Region:** Missouri **City:** Saint Louis **Latitude:** 38.707321 **Longitude:** -90.303543 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 142.250.72.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
any.example.com	ok	No Geolocation information available.
esi-drupal-cdn-prod.s3.amazonaws.com	ok	**IP:** 54.231.201.129 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
www.quallentpharmaceuticals.com	ok	**IP:** 18.238.96.4 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
clientsdk.launchdarkly.com	ok	**IP:** 151.101.1.55 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
p1.login.accredo.com	ok	**IP:** 3.221.83.4 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.hhs.gov	ok	**IP:** 2.19.158.16 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
youtrack.jetbrains.com	ok	**IP:** 63.33.88.220 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
tools.usps.com	ok	**IP:** 23.222.205.99 **Country:** United States of America **Region:** Minnesota **City:** Minneapolis **Latitude:** 44.979969 **Longitude:** -93.263840 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
mobile.launchdarkly.com	ok	**IP:** 23.20.148.186 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
api3-eu.branch.io	ok	**IP:** 18.155.173.13 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.express-scripts.com	ok	**IP:** 167.211.52.57 **Country:** United States of America **Region:** New Jersey **City:** Franklin Lakes **Latitude:** 41.009102 **Longitude:** -74.208122 **View:** Google Map
www.accredo.com	ok	**IP:** 18.155.173.104 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www-dev.accredo.acdo	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
express-scripts.calculator.m3p.health	ok	**IP:** 18.238.109.29 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
cdn.branch.io	ok	**IP:** 18.238.109.76 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www-qa.express-scripts.com	ok	No Geolocation information available.
clientstream.launchdarkly.com	ok	**IP:** 76.223.31.44 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
ocrportal.hhs.gov	ok	**IP:** 156.40.11.174 **Country:** United States of America **Region:** Maryland **City:** Bethesda **Latitude:** 38.999641 **Longitude:** -77.155083 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.mongodb.com	ok	**IP:** 15.197.167.90 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.fedex.com	ok	**IP:** 23.62.226.165 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
realm.io	ok	**IP:** 13.224.53.92 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
api2.branch.io	ok	**IP:** 18.238.109.16 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
assets.adobedtm.com	ok	**IP:** 23.3.85.32 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
accredo-50845.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.medicare.gov	ok	**IP:** 23.32.109.213 **Country:** Sweden **Region:** Stockholms lan **City:** Stockholm **Latitude:** 59.332581 **Longitude:** 18.064899 **View:** Google Map
goo.gle	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map

EMAILS

EMAIL	FILE
test@gmail.com	o6/b.java
u0013android@android.com0 u0013android@android.com	dc/t.java
accredorxhelp@accredo.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Adobe Experience Cloud		https://reports.exodus-privacy.eu.org/trackers/229

HARDCODED SECRETS

POSSIBLE SECRETS
"common_password" : "Password"
"common_username" : "Username"
"firebase_database_url" : "https://accredo-50845.firebaseio.com"

POSSIBLE SECRETS
"google_api_key" : "AIzaSyDAyd_JjcKLEJr7YktEWWSFFGCjxXnRQAY"
"google_crash_reporting_api_key" : "AIzaSyDAyd_JjcKLEJr7YktEWWSFFGCjxXnRQAY"
000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F808182838485868788898A8B8C8D8E8F909192939495969798999A9B9C9D9E9FA0A1A2A3A4A5A6A7A8A9AAABACADAEAFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBFC0C1C2C3C4C5C6C7C8C9CACBCCCDCECFD0D1D2D3D4D5D6D7D8D9DADBDCDDDEDFE0E1E2E3E4E5E6E7E8E9EAEBECEDEEEFF0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
b-bca32bf7-d13c-44ac-bd0c-14234503f341
70c1cafb-9bad-4802-8319-247305e69292

PLAYSTORE INFORMATION

Title: Accredo

Score: 4.680328 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.accredohealth.accredo

Developer Details: Accredo Health Group, Inc, Accredo+Health+Group,+Inc, None, http://accredo.com, accredoapp@accredo.com,

Release Date: Nov 16, 2017 **Privacy Policy:** Privacy link

Description:

The Accredo® mobile app offers Accredo patients the convenience of managing specialty medications how you want, when you want. With the Accredo mobile app, you can: • Order specialty medication refills* • Track your Accredo orders • Make payments • View specialty medication order history • Receive and track specialty medication dose reminders • Update your patient profile • Manage communication preferences • Contact Accredo with any questions *Not available for all specialty medications.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 18:56:11	Generating Hashes	OK
2025-08-29 18:56:11	Extracting APK	OK
2025-08-29 18:56:11	Unzipping	OK
2025-08-29 18:56:12	Parsing APK with androguard	OK
2025-08-29 18:56:12	Extracting APK features using aapt/aapt2	OK
2025-08-29 18:56:12	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 18:56:14	Parsing AndroidManifest.xml	OK
2025-08-29 18:56:14	Extracting Manifest Data	OK
2025-08-29 18:56:14	Manifest Analysis Started	OK
2025-08-29 18:56:14	Reading Network Security config from security_config.xml	OK

2025-08-29 18:56:14	Parsing Network Security config	OK
2025-08-29 18:56:14	Performing Static Analysis on: Accredo (com.accredohealth.accredo)	OK
2025-08-29 18:56:15	Fetching Details from Play Store: com.accredohealth.accredo	OK
2025-08-29 18:56:15	Checking for Malware Permissions	OK
2025-08-29 18:56:15	Fetching icon path	OK
2025-08-29 18:56:16	Library Binary Analysis Started	OK
2025-08-29 18:56:16	Reading Code Signing Certificate	OK
2025-08-29 18:56:16	Running APKiD 2.1.5	OK
2025-08-29 18:56:18	Detecting Trackers	OK
2025-08-29 18:56:20	Decompiling APK to Java with JADX	OK
2025-08-29 18:56:34	Converting DEX to Smali	OK

2025-08-29 18:56:34	Code Analysis Started on - java_source	OK
2025-08-29 18:56:36	Android SBOM Analysis Completed	OK
2025-08-29 18:56:41	Android SAST Completed	OK
2025-08-29 18:56:41	Android API Analysis Started	OK
2025-08-29 18:56:47	Android API Analysis Completed	OK
2025-08-29 18:56:47	Android Permission Mapping Started	OK
2025-08-29 18:56:52	Android Permission Mapping Completed	OK
2025-08-29 18:56:52	Android Behaviour Analysis Started	OK
2025-08-29 18:57:01	Android Behaviour Analysis Completed	OK
2025-08-29 18:57:01	Extracting Emails and URLs from Source Code	OK
2025-08-29 18:57:04	Email and URL Extraction Completed	OK

2025-08-29 18:57:04	Extracting String data from APK	OK
2025-08-29 18:57:04	Extracting String data from Code	OK
2025-08-29 18:57:04	Extracting String values and entropies from Code	OK
2025-08-29 18:57:08	Performing Malware check on extracted domains	OK
2025-08-29 18:57:14	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.