



ANDROID STATIC ANALYSIS REPORT

app_icon

 Ambetter (1.24.1122)

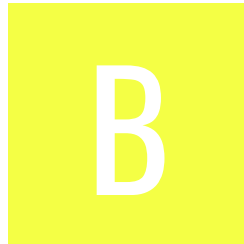
File Name: com.centene.dxe.ambetter_4992558.apk

Package Name: com.centene.dxe.ambetter

Scan Date: Aug. 29, 2025, 9:09 p.m.






App Security Score: 55/100 (MEDIUM RISK)

Grade:



Trackers Detection: 2/432

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
1	14	3	2	1

FILE INFORMATION

File Name: com.centene.dxe.ambetter_4992558.apk

Size: 17.19MB

MD5: adbd689a2ab2f7f3314faa3dedd52bb1

SHA1: 5784424b2a9c02bf82cc229a8a7c2c959e967cb2

SHA256: 8edcf23dae51300fe757e21c2a574005202496f3c50e317af51a996862f6b556

APP INFORMATION

App Name: Ambetter

Package Name: com.centene.dxe.ambetter

Main Activity: com.centene.person.iambetter.MainActivity

Target SDK: 34

Min SDK: 24

Max SDK:

Android Version Name: 1.24.1122

Android Version Code: 4992558

APP COMPONENTS

Activities: 10

Services: 6

Receivers: 10

Providers: 4

Exported Activities: 1

Exported Services: 1

Exported Receivers: 1

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed

v1 signature: False

v2 signature: True

v3 signature: True

v4 signature: False

X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2024-04-12 15:48:59+00:00

Valid To: 2054-04-12 15:48:59+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0x57072d6644cad832689a01853b3ac09361f3ad0f

Hash Algorithm: sha256

md5: bf9530524badc51983c28e6eb416460e

sha1: a578d84b2905a1b327d93e466d4b89837f350314

sha256: 29ced309a289122a7b213e4c875b3a445c764f71531d0d9207c03169d724f895

sha512: a21beafb3fc369c3e8cce12439e496957f7b4904a1fe413c87aae449bcbfaa4f1e499aaf678a9c15a77a5b486ca34aaf4bc0efa033b08f5eee9c714f4a4d81fa

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 9d3523c574f8e9a477df442dc03abaaa303ca3e6211dc3362b839b8075bd2dd8

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_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.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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
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.centene.dxe.ambetter.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.

FILE	DETAILS	
adbd689a2ab2f7f3314faa3dedd52bb1.apk	FINDINGS	DETAILS
	Anti-VM Code	possible VM check
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check network operator name check possible VM check
	Compiler	r8 without marker (suspicious)
classes2.dex	FINDINGS	DETAILS
	Compiler	r8 without marker (suspicious)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.centene.person.iambetter.MainActivity	Schemes: iambetter:///, Hosts: com.centene.dxe.ambetter, Paths: /auth/callback,
net.openid.appauth.RedirectUriReceiverActivity	Schemes: iambetter://,

NETWORK SECURITY

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: 3 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	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.
3	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.
4	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.

</> CODE ANALYSIS

HIGH: 0 | WARNING: 9 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a9/f.java b1/j.java b5/f.java b9/q0.java bb/a.java c0/c.java c9/e.java com/adobe/marketing/mobile/assurance/c.j ava com/adobe/marketing/mobile/reactnative/e dge/b.java com/amplitude/reactnative/c.java com/centene/person/iambetter/MainActivit y.java com/github/barteksc/pdfviewer/e.java com/github/barteksc/pdfviewer/h.java com/horcrux/svg/p.java com/learnium/RNDeviceInfo/RNDeviceMod ule.java com/learnium/RNDeviceInfo/e.java com/lugg/RNCCConfig/RNCCConfigModule.jav a com/oblador/keychain/KeychainModule.jav a com/reactnativecommunity/asyncstorage/g. java com/reactnativecommunity/cookies/Cookie ManagerModule.java com/reactnativecommunity/geolocation/q.j ava com/reactnativecommunity/webview/f.java com/reactnativecommunity/webview/j.java com/reactnativecommunity/webview/l.java com/rnfs/c.java com/rnmaps/maps/MapTileWorker.java com/rnmaps/maps/i.java com/rnmaps/maps/p.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/rnmaps/maps/q.java com/rnmaps/maps/s.java com/rnziparchive/RNZipArchiveModule.java com/swmansion/gesturehandler/react/RNGestureHandlerModule.java com/swmansion/gesturehandler/react/j.java com/swmansion/gesturehandler/react/k.java com/swmansion/reanimated/NativeMethodHelper.java com/swmansion/reanimated/ReanimatedModule.java com/swmansion/reanimated/ReanimatedUIManagerFactory.java com/swmansion/reanimated/layoutReanimation/AnimationsManager.java com/swmansion/reanimated/layoutReanimation/ReanimatedNativeHierarchyManager.java com/swmansion/reanimated/layoutReanimation/SharedTransitionManager.java com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/th3rdwave/safeareacontext/k.java db/c.java db/h.java db/i.java db/k.java e9/a.java eb/c.java eb/f.java f2/a.java f3/d.java fr/greweb/reactnativeviewshot/RNViewShotModule.java fr/greweb/reactnativeviewshot/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				h9/h.java h9/j.java i8/k.java i8/l.java i8/o.java i8/v.java i8/z.java io/legere/pdfiumandroid/DefaultLogger.java io/legere/pdfiumandroid/PdfiumCore.java j5/d.java j8/c0.java k8/a.java k8/b0.java k8/c.java k8/d1.java k8/e0.java k8/h1.java k8/q0.java k8/t0.java k8/u0.java k8/v0.java k8/x0.java l0/d.java n1/a.java n1/d.java n8/b.java nb/h.java nd/a.java o1/h.java o1/o.java o7/a.java o8/c.java o8/g.java org/wonday/pdf/a.java p1/a.java pd/c.java r0/c.java r8/h.java s/f.java s8/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				sa/i.java ua/n.java ua/p.java v0/a.java v9/d.java w0/m0.java w9/b.java x7/k.java y7/a.java y9/g.java yb/b.java z/f.java
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/amplitude/reactnative/AmplitudeReactNativeModule.java com/centene/person/iambetter/BuildConfig.java y2/c.java
3	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/ReactNativeBlobUtil/c.java com/learnium/RNDeviceInfo/RNDeviceInfoModule.java com/reactnativecommunity/webview/l.java com/rnfs/RNFSManager.java g4/a.java s1/c.java w3/a.java
4	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/ReactNativeBlobUtil/a.java com/reactnativecommunity/webview/l.java com/rnmaps/maps/MapModule.java com/rnmaps/maps/a.java fr/greweb/reactnativeviewshot/RNViewShotModule.java w3/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	ce/d.java ce/h.java od/z.java se/d.java ua/o.java w2/a.java w2/b.java
6	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	c8/b0.java c8/f0.java c8/h0.java com/reactnativemcommunity/asyncstorage/j.j ava s0/a.java x1/b.java x2/c.java x2/e.java y1/g.java
7	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	le/e.java oe/b.java p1/a.java pe/k.java pe/z.java qe/g.java t6/a.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/adobe/marketing/mobile/assurance/i0. java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	nb/h.java s2/b.java yd/c.java yd/d.java yd/i.java yd/j.java
10	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/ReactNativeBlobUtil/i.java
11	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	com/reactnativecommunity/clipboard/ClipboardModule.java
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	com/reactnativecommunity/clipboard/ClipboardModule.java
13	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	q2/h.java
14	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	j4/c.java

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	a2/d.java com/ReactNativeBlobUtil/a.java com/ReactNativeBlobUtil/c.java com/ReactNativeBlobUtil/e.java com/ReactNativeBlobUtil/h.java com/reactnativecommunity/asyncstorage/g.java com/rnfs/RNFSManager.java com/rnfs/i.java com/rnmaps/maps/a.java com/rnmaps/maps/k.java com/rnmaps/maps/p.java de/r.java h2/b.java ic/m.java id/a.java jd/b.java je/y1.java p0/c.java u3/b.java v6/a.java x5/d.java y1/c.java
00078	Get the network operator name	collection telephony	com/adobe/marketing/mobile/assurance/c.java com/amplitude/reactnative/a.java com/learnium/RNDeviceInfo/RNDeviceModule.java e3/a.java f2/i.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/ReactNativeBlobUtil/d.java com/ReactNativeBlobUtil/g.java com/adobe/marketing/mobile/LocalNotificationHandler.java com/adobe/marketing/mobile/assurance/AssuranceExtension.java com/rnappauth/RNAppAuthModule.java io/swan/rnbrowser/a.java j2/a.java k8/k1.java n1/a.java net/openid/appauth/c.java o1/h.java o1/o.java o7/a.java yb/b.java
00022	Open a file from given absolute path of the file	file	a4/c.java com/ReactNativeBlobUtil/c.java com/ReactNativeBlobUtil/g.java com/oblador/vectoricons/a.java com/rnfs/RNFSManager.java ed/h.java fr/greweb/reactnativeviewshot/RNViewShotModule.java g4/a.java id/a.java id/d.java n1/d.java n1/f.java n1/g.java p0/a.java s0/b.java s1/c.java w3/f.java y1/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/ReactNativeBlobUtil/g.java com/adobe/marketing/mobile/LocalNotificationHandler.java j2/a.java k8/k1.java o1/h.java
00024	Write file after Base64 decoding	reflection file	com/ReactNativeBlobUtil/a.java com/ReactNativeBlobUtil/g.java n1/f.java n1/g.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00130	Get the current WIFI information	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00134	Get the current WiFi IP address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceModule.java
00096	Connect to a URL and set request method	command network	com/adobe/marketing/mobile/assurance/a.java
00089	Connect to a URL and receive input stream from the server	command network	com/adobe/marketing/mobile/assurance/a.java com/rnfs/c.java r2/a.java ua/n.java
00109	Connect to a URL and get the response code	network command	com/adobe/marketing/mobile/assurance/a.java com/rnfs/c.java r2/a.java ua/n.java

RULE ID	BEHAVIOUR	LABEL	FILES
00153	Send binary data over HTTP	http	com/adobe/marketing/mobile/assurance/a.java
00009	Put data in cursor to JSON object	file	com/amplitude/reactnative/b.java com/reactnativecommunity/asyncstorage/a.java
00036	Get resource file from res/raw directory	reflection	com/rnmaps/maps/d.java com/rnmaps/maps/l.java j7/a.java n1/d.java
00189	Get the content of a SMS message	sms	j4/f.java s1/c.java
00188	Get the address of a SMS message	sms	j4/f.java s1/c.java
00200	Query data from the contact list	collection contact	j4/f.java s1/c.java
00201	Query data from the call log	collection callog	j4/f.java s1/c.java
00147	Get the time of current location	collection location	com/reactnativecommunity/geolocation/a.java com/reactnativecommunity/geolocation/q.java
00075	Get location of the device	collection location	com/reactnativecommunity/geolocation/a.java
00079	Hide the current app's icon	evasion	k1/f.java
00192	Get messages in the SMS inbox	sms	com/rnfs/RNFSManager.java n1/d.java s1/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/rnfs/RNFSManager.java
00028	Read file from assets directory	file	com/rnfs/RNFSManager.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/rnfs/RNFSManager.java s1/c.java
00162	Create InetAddress object and connecting to it	socket	yd/b.java yd/j.java
00163	Create new Socket and connecting to it	socket	f2/q.java yd/b.java yd/j.java
00123	Save the response to JSON after connecting to the remote server	network command	net/openid/appauth/h.java
00132	Query The ISO country code	telephony collection	com/amplitude/reactnative/a.java
00012	Read data and put it into a buffer stream	file	com/rnfs/i.java
00114	Create a secure socket connection to the proxy address	network command	td/f.java
00094	Connect to a URL and read data from it	command network	c9/i0.java
00091	Retrieve data from broadcast	collection	com/ReactNativeBlobUtil/g.java com/adobe/marketing/mobile/LocalNotificationHandler.java net/openid/appauth/AuthorizationManagementActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00125	Check if the given file path exist	file	com/ReactNativeBlobUtil/g.java
00191	Get messages in the SMS inbox	sms	com/ReactNativeBlobUtil/g.java s1/c.java
00043	Calculate WiFi signal strength	collection wifi	hb/e.java
00014	Read file into a stream and put it into a JSON object	file	v6/a.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/rnmaps/maps/p.java
00072	Write HTTP input stream into a file	command network file	com/rnfs/c.java
00030	Connect to the remote server through the given URL	network	com/rnfs/c.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	s1/c.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.INTERNET, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	3/44	com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, 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
bewellnm.com	ok	IP: 141.193.213.10 Country: United States of America Region: Texas City: Austin Latitude: 30.271158 Longitude: -97.741699 View: Google Map

DOMAIN	STATUS	GEOLOCATION
dynatracecag.centene.com	ok	IP: 204.107.62.176 Country: United States of America Region: Missouri City: Saint Louis Latitude: 38.645458 Longitude: -90.325737 View: Google Map
pinterest.com	ok	IP: 151.101.0.84 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
plus.google.com	ok	IP: 64.233.185.102 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
blobs.griffon.adobe.com	ok	No Geolocation information available.
sso.entrykeyid.com	ok	IP: 35.155.99.122 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map

DOMAIN	STATUS	GEOLOCATION
centene.az1.qualtrics.com	ok	IP: 23.202.57.104 Country: United States of America Region: California City: San Jose Latitude: 37.339390 Longitude: -121.894958 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
device.griffon.adobe.com	ok	IP: 13.224.53.59 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
external-api-mobile.my.centene.com	ok	IP: 52.22.221.170 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	IP: 140.82.113.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
twitter.com	ok	IP: 172.66.0.227 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
docs.swmansion.com	ok	IP: 104.21.27.136 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
www.example.com	ok	IP: 23.220.73.43 Country: Colombia Region: Antioquia City: Medellin Latitude: 6.251840 Longitude: -75.563591 View: Google Map

DOMAIN	STATUS	GEOLOCATION
member.ambetterhealth.com	ok	IP: 18.238.96.117 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
ns.adobe.com	ok	No Geolocation information available.
enroll.ambetterhealth.com	ok	IP: 3.213.17.254 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
assets.adobedtm.com	ok	IP: 72.247.97.53 Country: United States of America Region: California City: Los Angeles Latitude: 34.052231 Longitude: -118.243683 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

DOMAIN	STATUS	GEOLOCATION
www.moneygram.com	ok	IP: 107.154.75.165 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map
www.teladoc.com	ok	IP: 104.17.31.172 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	i8/u.java
place_member_support@centene.com	com/centene/person/iambetter/BuildConfig.java
place_member_support@centene.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Adobe Experience Cloud		https://reports.exodus-privacy.eu.org/trackers/229
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125

HARDCODED SECRETS

POSSIBLE SECRETS
"AMPLITUDE_API_KEY" : "d9bb953881c2e164acd1ad1f954d74b3"
"CORRELATION_HEADER_KEY" : "X-CorrelationID"
"EKID_AUTH_URL" : "https://sso.entrykeyid.com/as/authorization.oauth2"
"EKID_END_SESSION_URL" : "https://sso.entrykeyid.com/idp/startSLO.ping"
"EKID_TOKEN_REVOCATION_URL" : "https://sso.entrykeyid.com/as/revoke_token.oauth2"
"EKID_TOKEN_URL" : "https://sso.entrykeyid.com/as/token.oauth2"
"GOOGLE_PLACES_API_KEY_ANDROID" : "AlzaSyB-Nt96dXqcQvA_UPj-pDTxBb_G81ipj5w"
"GOOGLE_PLACES_API_KEY_IOS" : "AlzaSyA_j0ruNGUaT_VmUnCGJkXESMXsLtdju6M"
"OE_HEADER_KEY" : "oe_next_plan_year"
c103703e120ae8cc73c9248622f3cd1e

POSSIBLE SECRETS
88c5d9ae-adbb-49a7-a953-4bff5875a320
ABi2fbt8vkzj7SJ8aD5jc4xJFTDFntdkMrYXL3itsvqY1Qlw
000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F808182838485868788898A8B8C8D8E8F909192939495969798999A9B9C9D9E9FA0A1A2A3A4A5A6A7A8A9AAABACADAEAFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBFC0C1C2C3C4C5C6C7C8C9CACBCCCDCECFD0D1D2D3D4D5D6D7D8D9DADBDCDDDEDFE0E1E2E3E4E5E6E7E8E9EAEBECEDEEEFF0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF
2a86ebf9-1390-4df6-ba72-a7091f293ec5
e1798ff6-169d-45c2-a887-b58bee6def0c
dZozdop5rgKNxjbrQAd5nntAGpgh9w84O1Xgg==
258EAFa5-E914-47DA-95CA-C5AB0DC85B11
7fmduHKTdHHrIMvldIEqAllSfii1tl35bxj1OXN5Ve8c4IU6URVu4xtSHc3BVZxS6WWJnxMDhIfQN0N0K2NDJg==
49f946663a8deb7054212b8adda248c6
d9bb953881c2e164acd1ad1f954d74b3

PLAYSTORE INFORMATION

Title: Ambetter Health

Score: 4.4198895 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** [com.centene.dxe.ambetter](https://play.google.com/store/apps/details?id=com.centene.dxe.ambetter)

Developer Details: Centene Corporation, 8472307307058117449, None, None, SM_dxe_mobile_marketplace_member_support@centene.com,

Description:

Manage your healthcare benefits on the go with the Ambetter Health mobile app.† Sign in to your current account or create a new account to easily and securely access the information you need. • View, save, and share ID card • Find care: View current primary care provider (PCP) ; Search for in-network doctors, specialists, hospitals, and clinics near you • Pay premium and view payment history • Get answers to your questions; View FAQs; Contact member support • View covered services and benefits usage, including deductible and maximum out-of-pocket amounts † Ambetter Health is the brand name used for products and services provided by one or more of the wholly owned subsidiaries of Centene Corporation, who are Qualified Health Plan issuers in the states indicated at ambetterhealthAmbetterHealth.com. Health benefits and health insurance plans contain exclusions and limitations. ©2025 Centene Corporation, centene.com. All rights reserved. For information on your right to receive an Ambetter Health plan free of discrimination, or your right to receive language, auditory and/or visual assistance services, please visit ambetterhealth.com and scroll to the bottom of the page.

☰ SCAN LOGS

Timestamp	Event	Error
2025-08-29 21:09:00	Generating Hashes	OK
2025-08-29 21:09:00	Extracting APK	OK
2025-08-29 21:09:00	Unzipping	OK
2025-08-29 21:09:00	Parsing APK with androguard	OK
2025-08-29 21:09:00	Extracting APK features using aapt/aapt2	OK

2025-08-29 21:09:00	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 21:09:02	Parsing AndroidManifest.xml	OK
2025-08-29 21:09:02	Extracting Manifest Data	OK
2025-08-29 21:09:02	Manifest Analysis Started	OK
2025-08-29 21:09:02	Performing Static Analysis on: Ambetter (com.centene.dxe.ambetter)	OK
2025-08-29 21:09:03	Fetching Details from Play Store: com.centene.dxe.ambetter	OK
2025-08-29 21:09:03	Checking for Malware Permissions	OK
2025-08-29 21:09:03	Fetching icon path	OK
2025-08-29 21:09:03	Library Binary Analysis Started	OK
2025-08-29 21:09:03	Reading Code Signing Certificate	OK
2025-08-29 21:09:04	Running APKiD 2.1.5	OK

2025-08-29 21:09:06	Detecting Trackers	OK
2025-08-29 21:09:08	Decompiling APK to Java with JADX	OK
2025-08-29 21:09:17	Converting DEX to Smali	OK
2025-08-29 21:09:17	Code Analysis Started on - java_source	OK
2025-08-29 21:09:19	Android SBOM Analysis Completed	OK
2025-08-29 21:09:25	Android SAST Completed	OK
2025-08-29 21:09:25	Android API Analysis Started	OK
2025-08-29 21:09:30	Android API Analysis Completed	OK
2025-08-29 21:09:30	Android Permission Mapping Started	OK
2025-08-29 21:09:35	Android Permission Mapping Completed	OK

2025-08-29 21:09:35	Android Behaviour Analysis Started	OK
2025-08-29 21:09:42	Android Behaviour Analysis Completed	OK
2025-08-29 21:09:42	Extracting Emails and URLs from Source Code	OK
2025-08-29 21:09:44	Email and URL Extraction Completed	OK
2025-08-29 21:09:44	Extracting String data from APK	OK
2025-08-29 21:09:44	Extracting String data from Code	OK
2025-08-29 21:09:44	Extracting String values and entropies from Code	OK
2025-08-29 21:09:45	Performing Malware check on extracted domains	OK
2025-08-29 21:09:47	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.

