ANDROID STATIC ANALYSIS REPORT

Vision Engage (3.10.0)

File Name:	com.vc.thedeepcentric_41.apk
Package Name:	com.vc.thedeepcentric
Scan Date:	Sept. 1, 2025, 11:08 a.m.
App Security Score:	56/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	8/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	12	3	2	1

FILE INFORMATION

File Name: com.vc.thedeepcentric_41.apk
Size: 16.65MB
MD5: 77970d0994915e91d87677255802f939
SHA1: 83390750c18c594ba38aef58cf549dd19aad9a3d
SHA256: 78e2c0e72b5de2c94862c73d31d8b5b57b3da4f5fdf64faafd61b0c01fc0594f

APP INFORMATION

App Name: Vision Engage
Package Name: com.vc.thedeepcentric
Main Activity: com.vc.thedeepcentric.activities.SplashScreenActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 3.10.0

Android Version Code: 41

APP COMPONENTS

Activities: 24
Services: 8
Receivers: 5
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: 2022-09-01 10:14:23+00:00
Valid To: 2052-09-01 10:14:23+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xaa83347c830ca02f560b980a5c8421b309f47f0
Hash Algorithm: sha256
md5: 67b95863d9bdbba0f8589b5971a68ded
sha1: 3d7e12489f47eaaa570434e12750bf6c5b699832
sha256: 2485ca396860626edbd31d267ac6d81d44d691057da91c7dd797dbe77916cfb9
sha512: 758f3c28ae5e84d823e424d52f3b47a14e86f1d1d0924191b7792b77798e0e64a976c9013b92aa2dcb6430a08a4be959fc5c8f1c908afc031ec6325709b9df1a
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 3c2abbb02b3f1887a3dec104f06347dd8f1285b9a237312fc993af9f497c1259
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.

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.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.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.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.vc.thedeepcentric.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
network operator name check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

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

<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>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>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.vc.thedeepcentric.activities.SplashScreenActivity	Schemes: deepcentric://, https://, Hosts: open, @string/host_name, @string/host_name_alternate,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.vc.thedeepcentric,

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: **0** | WARNING: **4** | 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	Activity (com.facebook.CustomTabActivity) 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
3	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
4	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.

CODE ANALYSIS

HIGH: **0** | WARNING: **7** | INFO: **3** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/amazonaws/cognito/clientcontext/data/UserContextDataProvider.java com/amazonaws/cognito/clientcontext/datacollection/ApplicationDataCollector.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ction/ApplicationDataCollector.java com/amazonaws/cognito/clientcontext/util/SignatureGenerator.java com/amazonaws/logging/AndroidLog.java com/amazonaws/logging/LogFactory.java com/amazonaws/mobile/auth/core/DefaultSignInResultHandler.java com/amazonaws/mobile/auth/core/IdentityManager.java com/amazonaws/mobile/auth/core/signin/SignInManager.java com/amazonaws/mobile/client/AWSMobileClient.java com/amazonaws/mobile/client/internal/InternalCallback.java com/amazonaws/mobile/client/internal/oauth2/OAuth2Client.java com/amazonaws/mobileconnectors/cognitoidentityprovider/CognitoUserSession.java com/amazonaws/services/chime/sdk/meetings/audiovideo/video/backgroundfilter/SegmentationProcessor.java com/amazonaws/services/chime/sdk/meetings/utils/logger/ConsoleLogger.java com/amplifyframework/hub/HubSubscriber.java com/amplifyframework/logging/AndroidLogger.java com/amplifyframework/logging/JavaLogger.java com/biba/bibacommon/ProxyConfig.java com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.j

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ava com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/ImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.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/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignature.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/fasterxml/jackson/core/util/VersionUtil.java com/fasterxml/jackson/databind/util/ISO8601Utils.java com/microsoft/cognitiveservices/speech/util/SafeHandle.java com/vc/thedeepcentric/BaseApp.java com/vc/thedeepcentric/activities/MainActivity.java com/vc/thedeepcentric/activities/PinViewActivity.java com/vc/thedeepcentric/activities/PreScreeningActivity.java com/vc/thedeepcentric/activities/SplashScreenActivity.java com/vc/thedeepcentric/activities/UserProfileActivity.java com/vc/thedeepcentric/activities/VPayWebViewActivity.java com/vc/thedeepcentric/network/RemoteApiRepository.java com/vc/thedeepcentric/network/TokenInterceptor.java com/vc/thedeepcentric/network/TokenProvider.java com/vc/thedeepcentric/services/CognitoValidationService.java com/vc/thedeepcentric/services/PushListenerService.java com/vc/thedeepcentric/ui/main/MedicationsFragment.java com/vc/thedeepcentric/ui/main/OtpVerificationFragment.java com/vc/thedeepcentric/ui/main/PreScreeningQuestionsFragment$iterateToShow$1.java com/vc/thedeepcentric/ui/main/PreScreeningQuestionsFragment$submitSurveyApiCall$1.java com/vc/thedeepcentric/ui/main/PreScreeningQuestionsFragment.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/vc/thedeepcentric/ui/main/RaceFragment.java com/vc/thedeepcentric/ui/main/StudyDetailsFragment.java com/vc/thedeepcentric/ui/main/SubmitSurveyFragment.java com/vc/thedeepcentric/ui/main/SuccessMessageMedicalDetailsFragment.java com/vc/thedeepcentric/utils/AppRatingHelper.java com/vc/thedeepcentric/utils/AzureVoiceToText.java com/vc/thedeepcentric/utils/FeedbackDialog.java com/vc/thedeepcentric/utils/Utils.java com/vc/thedeepcentric/viewmodel/PreScreeningViewModel.java com/vc/thedeepcentric/viewmodel/SearchViewModel.java com/vc/thedeepcentric/viewmodel/SocialServices.java com/vc/thedeepcentric/viewmodel/VoiceRecordingViewModel.java com/xodee/client/audio/audioclient/AudioClient.java com/yalantis/ucrop/UCropActivity.java com/yalantis/ucrop/task/BitmapCropTask.java com/yalantis/ucrop/task/BitmapLoadTask.java com/yalantis/ucrop/util/BitmapLoadUtils.java com/yalantis/ucrop/util/EglUtils.java com/yalantis/ucrop/util/FileUtils.java com/yalantis/ucrop/util/ImageHeaderParser.java com/yalantis/ucrop/view/TransformImageView.java io/branch/referral/BranchJsonConfig.java io/branch/referral/BranchLogger.java io/branch/referral/validators/IntegrationValidator.java org/jsoup/examples/HtmlToPlainText.java org/jsoup/examples/ListLinks.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/amazonaws/auth/CognitoCachingCredentialsProvider.java com/amazonaws/auth/policy/conditions/ConditionFactory.java com/amazonaws/cognito/clientcontext/data/UserContextDataProvider.java com/amazonaws/cognito/clientcontext/datacollection/DeviceDataCollector.java com/amazonaws/internal/keyvaluestore/AWSKeyValueStore.java com/amazonaws/internal/keyvaluestore/KeyProvider18.java com/amazonaws/mobile/auth/core/IdentityManager.java com/amazonaws/mobile/client/AWSMobileClient.java com/amazonaws/mobile/client/internal/oauth2/OAuth2Client.java com/amazonaws/mobileconnectors/cognitoidentityprovider/util/CognitoDeviceHelper.java com/amazonaws/mobileconnectors/cognitoidentityprovider/util/CognitoPinpointSharedContext.java com/amazonaws/mobileconnectors/cognitoidentityprovider/util/CognitoServiceConstants.java com/amazonaws/mobileconnectors/pinpoint/analytics/SessionClient.java com/amazonaws/mobileconnectors/pinpoint/internal/core/configuration/AndroidPreferencesConfiguration.java com/amazonaws/mobileconnectors/pinpoint/internal/core/idresolver/SharedPrefsUniqueIdService.java com/amazonaws/mobileconnectors/pinpoint/internal/event/ClientContext.java com/amazonaws/mobileconnectors/pinpoint/internal/event/EventRecorder.java com/amazonaws/mobileconnectors/pinpoint/targeting/TargetingClient.java com/amazonaws/mobileconnectors/pinpoint/tar

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	geting/notification/NotificationClient.java com/amazonaws/mobileconnectors/pinpoint/targeting/notification/NotificationClientBase.java com/amazonaws/services/chime/sdk/meetings/internal/ingestion/IngestionEventConverter.java com/amazonaws/services/chime/sdk/meetings/internal/video/TURNCredentials.java com/amplifyframework/api/aws/ApiGraphQLRequestOptions.java com/amplifyframework/api/aws/AppSyncSigV4SignerInterceptorFactory.java com/amplifyframework/api/aws/GsonGraphQLResponseFactory.java com/amplifyframework/api/aws/SubscriptionAuthorizer.java com/amplifyframework/api/aws/sigv4/AppSyncSigV4SignerInterceptor.java com/amplifyframework/api/aws/sigv4/DefaultCognitoUserPoolsAuthProvider.java com/amplifyframework/api/graphql/GsonResponseAdapters.java com/amplifyframework/auth/AuthProvider.java com/amplifyframework/auth/AuthUser.java com/amplifyframework/auth/AuthUserAttribute.java com/amplifyframework/auth/AuthUserAttributeKey.java com/amplifyframework/core/category/CategoryConfiguration.java com/amplifyframework/storage/StorageItem.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/manager/RequestManagerRetriever.java com/vc/thedeepcentric/models/Data.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/vc/thedeepcentric/ui/main/PreScreeningQuestionsFragment.java com/vc/thedeepcentric/ui/main/SchedulingFragment.java com/vc/thedeepcentric/ui/main/SubmitSurveyFragment.java io/branch/referral/Branch.java io/branch/referral/BranchPreinstall.java io/branch/referral/DeferredAppLinkDataHandler.java io/branch/referral/PrefHelper.java io/branch/referral/ServerRequest.java io/branch/referral/ServerRequestQueue.java io/branch/referral/UniversalResourceAnalyser.java io/branch/referral/validators/DeepLinkRoutingValidator.java io/jsonwebtoken/JwsHeader.java org/jsoup/nodes/Comment.java org/jsoup/nodes/DataNode.java org/jsoup/nodes/TextNode.java org/jsoup/nodes/XmlDeclaration.java
3	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/amazonaws/mobileconnectors/cognitoidentityprovider/CognitoUser.java com/amazonaws/mobileconnectors/cognitoidentityprovider/util/CognitoDeviceHelper.java dev/gustavoavila/websocketclient/WebSocketClient.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/vc/thedeepcentric/network/BuildUrl.java org/jsoup/helper/HttpConnection.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	com/amazonaws/mobileconnectors/pinpoint/targeting/notification/NotificationClientBase.java com/amazonaws/retry/PredefinedRetryPolicies.java dev/gustavoavila/websocketclient/WebSocketClient.java org/jsoup/helper/DataUtil.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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/amazonaws/util/Md5Utils.java
7	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/yalantis/ucrop/util/FileUtils.java
8	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	com/amazonaws/mobileconnectors/pinpoint/internal/event/EventTable.java com/amazonaws/mobileconnectors/pinpoint/internal/event/PinpointDBBase.java com/amazonaws/mobileconnectors/pinpoint/internal/event/PinpointDatabaseHelper.java com/amazonaws/services/chime/sdk/meetings/internal/ingestion/database/SQLiteDatabaseManager.java
9	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/amplifyframework/devmenu/DeveloperMenu.java io/branch/referral/ShareLinkManager.java
10	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/vc/thedeepcentric/utils/SharedPreferenceUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/vc/thedeepcentric/activities/VPayWebViewActivity.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/vc/thedeepcentric/ui/main/MedicationsFragment.java
00078	Get the network operator name	collection telephony	com/amazonaws/cognito/clientcontext/datacollection/TelephonyDataCollector.java com/amazonaws/mobileconnectors/pinpoint/internal/core/system/AndroidSystem.java io/branch/referral/SystemObserver.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/amazonaws/auth/PropertiesCredentials.java com/amazonaws/internal/ReleasableInputStream.java com/amazonaws/internal/ResettableInputStream.java com/amazonaws/mobileconnectors/pinpoint/internal/core/system/FileManager.java com/amazonaws/regions/RegionUtils.java com/amazonaws/util/Md5Utils.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/model/FileLoader.java com/fasterxml/jackson/core/JsonFactory.java com/fasterxml/jackson/databind/ObjectReader.java com/microsoft/cognitiveservices/speech/KeywordRecognitionModel.java com/yalantis/ucrop/util/FileUtils.java okio/Okio__JvmOkioKt.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/amazonaws/mobile/client/AWSMobileClient.java com/amazonaws/mobileconnectors/pinpoint/targeting/notification/NotificationClientBase.java com/amplifyframework/devmenu/DevMenuFileIssueFragment.java com/vc/thedeepcentric/ui/main/MedicationsFragment.java com/vc/thedeepcentric/ui/main/WebviewFragment.java com/vc/thedeepcentric/utils/Utils.java io/branch/referral/Branch.java io/branch/referral/validators/DeepLinkRoutingValidator.java
00091	Retrieve data from broadcast	collection	com/amazonaws/mobileconnectors/pinpoint/targeting/notification/NotificationDetails.java com/vc/thedeepcentric/activities/LanguageSelectionActivity.java com/vc/thedeepcentric/activities/SplashScreenActivity.java io/branch/referral/Branch.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/amazonaws/mobileconnectors/pinpoint/targeting/notification/NotificationClientBase.java com/vc/thedeepcentric/utils/Utils.java io/branch/referral/Branch.java
00036	Get resource file from res/raw directory	reflection	com/amazonaws/mobileconnectors/pinpoint/internal/event/PinpointDBBase.java com/amazonaws/mobileconnectors/pinpoint/targeting/notification/NotificationClientBase.java com/vc/thedeepcentric/utils/Utils.java io/branch/referral/Branch.java
00112	Get the date of the calendar event	collection calendar	com/fasterxml/jackson/databind/ser/std/StdKeySerializers.java com/vc/thedeepcentric/utils/Utils.java
00096	Connect to a URL and set request method	command network	com/amazonaws/http/UrlHttpClient.java com/amazonaws/services/chime/sdk/meetings/internal/utils/HttpUtils$makePostRequest$2.java com/amazonaws/services/chime/sdk/meetings/internal/utils/TURNRequestUtils$doTurnRequest$2.java org/jsoup/helper/HttpConnection.java
00089	Connect to a URL and receive input stream from the server	command network	com/amazonaws/http/UrlHttpClient.java com/amazonaws/services/chime/sdk/meetings/internal/utils/HttpUtils$makePostRequest$2.java com/amazonaws/services/chime/sdk/meetings/internal/utils/TURNRequestUtils$doTurnRequest$2.java com/amazonaws/util/HttpUtils.java com/bumptech/glide/load/data/HttpUrlFetcher.java org/jsoup/helper/HttpConnection.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java org/jsoup/helper/HttpConnection.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/amazonaws/http/UrlHttpClient.java com/amazonaws/services/chime/sdk/meetings/internal/utils/HttpUtils$makePostRequest$2.java com/amazonaws/services/chime/sdk/meetings/internal/utils/TURNRequestUtils$doTurnRequest$2.java com/amazonaws/util/HttpUtils.java com/bumptech/glide/load/data/HttpUrlFetcher.java org/jsoup/helper/HttpConnection.java
00102	Set the phone speaker on	command	com/amazonaws/services/chime/sdk/meetings/device/DefaultDeviceController.java com/amazonaws/services/chime/sdk/meetings/internal/audio/DefaultAudioClientController.java
00056	Modify voice volume	control	org/amazon/chime/webrtc/audio/WebRtcAudioTrack.java org/amazon/chime/webrtc/voiceengine/WebRtcAudioTrack.java
00189	Get the content of a SMS message	sms	com/vc/thedeepcentric/ui/main/MedicationsFragment.java com/vc/thedeepcentric/utils/Utils.java
00022	Open a file from given absolute path of the file	file	com/amazonaws/auth/PropertiesCredentials.java com/fasterxml/jackson/databind/ser/std/FileSerializer.java com/vc/thedeepcentric/ui/main/MedicationsFragment.java org/jsoup/Jsoup.java
00188	Get the address of a SMS message	sms	com/vc/thedeepcentric/ui/main/MedicationsFragment.java com/vc/thedeepcentric/utils/Utils.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/vc/thedeepcentric/ui/main/MedicationsFragment.java com/vc/thedeepcentric/utils/Utils.java
00191	Get messages in the SMS inbox	sms	com/vc/thedeepcentric/ui/main/MedicationsFragment.java com/vc/thedeepcentric/utils/Utils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00200	Query data from the contact list	collection contact	com/vc/thedeepcentric/ui/main/MedicationsFragment.java com/vc/thedeepcentric/utils/Utils.java
00201	Query data from the call log	collection calllog	com/vc/thedeepcentric/ui/main/MedicationsFragment.java com/vc/thedeepcentric/utils/Utils.java
00208	Capture the contents of the device screen	collection screen	org/amazon/chime/webrtc/ScreenCapturerAndroid.java
00009	Put data in cursor to JSON object	file	com/amazonaws/mobileconnectors/pinpoint/internal/event/EventRecorder.java com/vc/thedeepcentric/utils/Utils.java
00023	Start another application from current application	reflection control	com/amazonaws/mobileconnectors/pinpoint/targeting/notification/NotificationClientBase.java
00183	Get current camera parameters and change the setting.	camera	org/amazon/chime/webrtc/Camera1Session.java
00162	Create InetSocketAddress object and connecting to it	socket	com/amplifyframework/core/reachability/SocketHost.java dev/gustavoavila/websocketclient/WebSocketClient.java
00163	Create new Socket and connecting to it	socket	com/amplifyframework/core/reachability/SocketHost.java dev/gustavoavila/websocketclient/WebSocketClient.java
00003	Put the compressed bitmap data into JSON object	camera	io/branch/referral/network/BranchRemoteInterfaceUrlConnection.java
00012	Read data and put it into a buffer stream	file	com/amazonaws/util/Md5Utils.java com/microsoft/cognitiveservices/speech/KeywordRecognitionModel.java
00192	Get messages in the SMS inbox	sms	com/yalantis/ucrop/util/FileUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00094	Connect to a URL and read data from it	command network	com/amazonaws/http/UrlHttpClient.java
00108	Read the input stream from given URL	network command	com/amazonaws/http/UrlHttpClient.java
00126	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/vc/thedeepcentric/utils/Utils.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/vc/thedeepcentric/utils/Utils.java
00025	Monitor the general action to be performed	reflection	com/vc/thedeepcentric/utils/Utils.java
00137	Get last known location of the device	location collection	com/vc/thedeepcentric/utils/Utils.java
00004	Get filename and put it to JSON object	file collection	com/vc/thedeepcentric/utils/Utils.java
00115	Get last known location of the device	collection location	com/vc/thedeepcentric/utils/Utils.java
00010	Read sensitive data(SMS, CALLLOG) and put it into JSON object	sms calllog collection	com/vc/thedeepcentric/utils/Utils.java
00113	Get location and put it into JSON	collection location	com/vc/thedeepcentric/utils/Utils.java
00016	Get location info of the device and put it to JSON object	location collection	com/vc/thedeepcentric/utils/Utils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00034	Query the current data network type	collection network	com/amazonaws/cognito/clientcontext/datacollection/TelephonyDataCollector.java
00065	Get the country code of the SIM card provider	collection	com/amazonaws/cognito/clientcontext/datacollection/TelephonyDataCollector.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/982395193499/namespaces/firebase:fetch?key=AIzaSyC3Hg1UuPz7Alhtbv8VMql4ZulPnsHAppU. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.ACCESS_COARSE_LOCATION, android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.READ_PHONE_STATE, android.permission.CAMERA, android.permission.SYSTEM_ALERT_WINDOW, android.permission.ACCESS_NETWORK_STATE, android.permission.RECORD_AUDIO, android.permission.WAKE_LOCK
Other Common Permissions	4/44	com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, android.permission.MODIFY_AUDIO_SETTINGS, 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
help.branch.io	ok	**IP:** 104.18.21.218 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.googleapis.com	ok	**IP:** 142.250.74.42 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
branch.app.link	ok	**IP:** 18.238.109.80 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.branch.io	ok	**IP:** 18.238.109.24 **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.
bnc.lt	ok	**IP:** 18.238.109.60 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
javax.xml.xmlconstants	ok	No Geolocation information available.
cdn.branch.io	ok	**IP:** 13.224.53.2 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
api2.branch.io	ok	**IP:** 18.238.96.12 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
velocity.nmible.net	ok	**IP:** 18.155.173.46 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
velocityclinicaltrials.eu	ok	**IP:** 104.21.112.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.velocityclinical.com	ok	**IP:** 107.23.107.26 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
velocityclinical.com	ok	**IP:** 104.26.15.251 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.amazon.com	ok	**IP:** 184.28.254.90 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **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

✉ EMAILS

EMAIL	FILE
velocityappsupport@velocityclinical.com	com/vc/thedeepcentric/utils/Utils.java
vision-feedback@velocityclinical.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Amazon Analytics (Amazon insights)	Analytics	https://reports.exodus-privacy.eu.org/trackers/95
Amazon Mobile Analytics (Amplify)	Analytics	https://reports.exodus-privacy.eu.org/trackers/423
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"api_timeout_limit" : "30"
"branch_io_key" : "key_live_cBbykNwclQ23UAS3KJxrAgajwtpqyv5o"
"cognito_client_secret" : "1anabu4uio8ifss0998d63tcf1sb3ntulfvune4b6utmj18r4s48"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"encryption_api_header" : "IGzpIgosZe3ndMwx1u6Yg6B1izqLiYNe9JuOFkx5"
"facebook_client_token" : "00a56bacbf6c2166a06bd98490fa9648"
"google_api_key" : "AIzaSyC3Hg1UuPz7Alhtbv8VMql4ZulPnsHAppU"
"google_client_secret" : "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"
"google_crash_reporting_api_key" : "AIzaSyC3Hg1UuPz7Alhtbv8VMql4ZulPnsHAppU"
"user_name" : "User"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A93AD2CAFFFFFFFFFFFFFFFF

POSSIBLE SECRETS
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa
515d6767-01b7-49e5-8273-c8d11b0f331d
e33866c6b021475b831e46d8dd06968f
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
c56fb7d591ba6704df047fd98f535372fea00211
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
9b8f518b086098de3d77736f9458a3d2f6f95a37
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
23c08176db1a47278d987cc220517518
cc2751449a350f668590264ed76692694a80308a
6b32400b-4551-47c6-8ee4-8e3862fd41b1

POSSIBLE SECRETS
04c589e5-9d39-486d-9418-b746cf441255
df6b721c8b4d3b6eb44c861d4415007e5a35fc95

PLAYSTORE INFORMATION

Title: Vision Engage

Score: 4.805128 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.vc.thedeepcentric

Developer Details: Velocity Clinical Research, Velocity+Clinical+Research, None, None, velocityappsupport@velocityclinical.com,

Release Date: Sep 28, 2022 **Privacy Policy:** Privacy link

Description:

Discover a new way to participate in clinical studies with VISION Engage — your gateway to the best clinical trial experience at Velocity Clinical Research! Whether you're a current participant or considering joining a study, VISION Engage brings the world of clinical trials to your fingertips. Elevate your experience with the following features: Explore New Studies: Instantly access a curated list of study opportunities tailored just for you. Build Your Profile: Keep your information up-to-date so VISION Engage can notify you when you may be eligible for a study. Faster payments: Seamlessly receive your study stipends via the app Manage Appointments: Never miss an important date with personalized notifications and reminders, ensuring you are always well-prepared for your upcoming visits. Stay in Touch: Stay connected with your Velocity site through seamless, in-app communication. Learn About Research: Navigate your clinical trial journey with ease, and gain insights into clinical trials, the diseases being studied, and more. Redefine your clinical study experience with VISION Engage by Velocity. Download the app now!

SCAN LOGS

Timestamp	Event	Error
2025-09-01 11:08:00	Generating Hashes	OK

2025-09-01 11:08:00	Extracting APK	OK
2025-09-01 11:08:00	Unzipping	OK
2025-09-01 11:08:01	Parsing APK with androguard	OK
2025-09-01 11:08:01	Extracting APK features using aapt/aapt2	OK
2025-09-01 11:08:01	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 11:08:03	Parsing AndroidManifest.xml	OK
2025-09-01 11:08:03	Extracting Manifest Data	OK
2025-09-01 11:08:03	Manifest Analysis Started	OK
2025-09-01 11:08:03	Performing Static Analysis on: Vision Engage (com.vc.thedeepcentric)	OK
2025-09-01 11:08:04	Fetching Details from Play Store: com.vc.thedeepcentric	OK
2025-09-01 11:08:06	Checking for Malware Permissions	OK

2025-09-01 11:08:06	Fetching icon path	OK
2025-09-01 11:08:06	Library Binary Analysis Started	OK
2025-09-01 11:08:06	Reading Code Signing Certificate	OK
2025-09-01 11:08:06	Running APKiD 2.1.5	OK
2025-09-01 11:08:11	Detecting Trackers	OK
2025-09-01 11:08:15	Decompiling APK to Java with JADX	OK
2025-09-01 11:08:33	Converting DEX to Smali	OK
2025-09-01 11:08:33	Code Analysis Started on - java_source	OK
2025-09-01 11:08:39	Android SBOM Analysis Completed	OK
2025-09-01 11:08:46	Android SAST Completed	OK
2025-09-01 11:08:46	Android API Analysis Started	OK

2025-09-01 11:08:54	Android API Analysis Completed	OK
2025-09-01 11:08:54	Android Permission Mapping Started	OK
2025-09-01 11:09:02	Android Permission Mapping Completed	OK
2025-09-01 11:09:03	Android Behaviour Analysis Started	OK
2025-09-01 11:09:10	Android Behaviour Analysis Completed	OK
2025-09-01 11:09:10	Extracting Emails and URLs from Source Code	OK
2025-09-01 11:09:14	Email and URL Extraction Completed	OK
2025-09-01 11:09:14	Extracting String data from APK	OK
2025-09-01 11:09:14	Extracting String data from Code	OK
2025-09-01 11:09:14	Extracting String values and entropies from Code	OK

2025-09-01 11:09:18	Performing Malware check on extracted domains	OK
2025-09-01 11:09:20	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.