MOBSF

ANDROID STATIC ANALYSIS REPORT

BCBSM (5.36.0)

File Name:	com.bcbsm.mmaprod_1713.apk
Package Name:	com.bcbsm.mmaprod
Scan Date:	Aug. 29, 2025, 8:07 p.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	22	4	3	1

FILE INFORMATION

File Name: com.bcbsm.mmaprod_1713.apk
Size: 26.14MB
MD5: a49a9d39760615747a29de1bbd321b44
SHA1: 4d82464cb8be954010622efb8a491c14555c6ab9
SHA256: 34689d7eb792e3e87ab980e6dc2862dc6e18d67245d7ee4374da3442b25966d8

APP INFORMATION

App Name: BCBSM
Package Name: com.bcbsm.mmaprod
Main Activity: com.bcbsm.mma.MainActivity
Target SDK: 34
Min SDK: 22
Max SDK:
Android Version Name: 5.36.0

Android Version Code: 1713

APP COMPONENTS

Activities: 17
Services: 15
Receivers: 18
Providers: 7
Exported Activities: 3
Exported Services: 2
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=MI, L=Detroit, O=BCBSM, OU=Digital Experience, CN=Gopala Molakaluri
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-11-18 20:36:14+00:00
Valid To: 2040-11-11 20:36:14+00:00
Issuer: C=US, ST=MI, L=Detroit, O=BCBSM, OU=Digital Experience, CN=Gopala Molakaluri
Serial Number: 0x3958280d
Hash Algorithm: sha256
md5: 1716baf58b264ab4f36bfc5242646357
sha1: 3ab1e209020fa1b53c39e18f2bce2a98d00ef82d
sha256: 7b0115906d44552e4e83626cb2b6bad171e37ba5ea2de480c01bab0b853ba1de
sha512: 7b55616f867bb86c023d06d47a4acf0f53c5711a4ca9f24febbddb0884ac903bdf7d42f69f8beaf33bb25f63e51c650e9233ec9911bf2fbcfafee0ad46131fef
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 8e4f1ed9496982afee485893e1301f11dd86f63bfb28fe8301b9192e26756baa
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
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_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.bcbsm.mmaprod.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
com.samsung.android.mapsagent.permission.READ_APP_INFO	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
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
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.TAGS check SIM operator check network operator name check ro.kernel.qemu check FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
possible Build.SERIAL check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.bcbsm.mma.MainActivity	Schemes: @string/custom_url_scheme://, bcbsmapp://,

NETWORK SECURITY

HIGH: 0 | WARNING: 2 | INFO: 0 | SECURE: 2

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	secure	Base config is configured to disallow clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.
3	bcbsm.com	secure	Domain config is securely configured to disallow clear text traffic to these domains in scope.
4	bcbsm.com	warning	Domain config is configured to trust system certificates.

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 9 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.1-5.1.1, [minSdk=22]	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	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Activity (com.verint.xm.sdk.predictive.tracker.app.invite.InviteActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (com.verint.xm.sdk.predictive.tracker.app.survey.SurveyActivity) 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
5	Activity (com.verint.xm.sdk.predictive.com.verint.xm.sdk.surveymanagement.survey.SurveyManagementActivity) 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.
6	TaskAffinity is set for activity (com.salesforce.marketingcloud.notifications.NotificationOpenActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
7	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected. [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.

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

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

NO	ISSUE	SEVERITY	DESCRIPTION
10	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
11	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: **2** | WARNING: **8** | INFO: **3** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/cap/browser/plugin/WebViewDialog.java com/capacitorjs/plugins/camera/CameraUtils.java com/capacitorjs/plugins/filesystem/Filesystem.java com/getcapacitor/BridgeWebChromeClient.java com/getcapacitor/FileUtils.java com/getcapacitor/plugin/http/FileExtensions.java com/verint/xm/sdk/common/LaunchArgumentsHelper.java
2	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/salesforce/marketingcloud/sfmcsdk/components/encryption/EncryptedSharedPreferences.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	capacitor/plugin/appsflyer/sdk/AppsFlyerConstantsKt.java com/capacitorjs/plugins/localnotifications/LocalNotificationManager.java com/capacitorjs/plugins/localnotifications/NotificationStorage.java com/capacitorjs/plugins/localnotifications/TimedNotificationPublisher.java com/getcapacitor/AppUUID.java com/getcapacitor/Bridge.java com/getcapacitor/Plugin.java com/ionicframework/IdentityVault/DevicePlugin.java com/ionicframework/auth/IonicCombinedVault.java com/ionicframework/auth/IonicSharedPreferenceVault.java com/ionicframework/auth/VaultFactory.java com/ionicframework/auth/VaultState.java com/okta/authfoundation/client/DeviceTokenProvider.java com/okta/authfoundation/credential/SharedPreferencesTokenStorage.java com/salesforce/marketingcloud/events/h.java com/verint/xm/sdk/common/environment/Environment.java net/gotev/cookiestore/SharedPreferencesCookieStore.java
				_COROUTINE/_BOUNDARY.java com/appsflyer/internal/AFg1aSDK.java com/bcbsm/plugins/okta/idx/CapOktaIdxPlugin.java com/bottlerocketstudios/vault/StandardSharedPreferenceVault.java com/bottlerocketstudios/vault/keys/generat

NO	ISSUE	SEVERITY	STANDARDS	FILES
				or/PbkdfKeyGenerator.java com/bottlerocketstudios/vault/keys/storage/CompatSharedPrefKeyStorageFactory.java com/bottlerocketstudios/vault/keys/storage/KeychainAuthenticatedKeyStorage.java com/bottlerocketstudios/vault/keys/storage/SharedPrefKeyStorage.java com/bottlerocketstudios/vault/keys/storage/hardware/AndroidKeystoreTester.java com/bottlerocketstudios/vault/keys/wrapper/ObfuscatingSecretKeyWrapper.java com/bottlerocketstudios/vault/salt/SaltBox.java com/cap/browser/plugin/CapBrowser.java com/codingsans/ionic/smsRetriever/AndroidSmsRetriever.java com/getcapacitor/Logger.java com/getcapacitor/community/inappreview/InAppReview.java com/getcapacitor/plugin/http/Http.java com/getcapacitor/plugin/http/cookie/CapacitorCookieManager.java com/ionicframework/IdentityVault/BiometricPromptActivity.java com/ionicframework/IdentityVault/Device.java com/ionicframework/IdentityVault/DeviceSecurityStrongVault.java com/ionicframework/IdentityVault/IdentityVaultPlugin.java com/ionicframework/IdentityVault/NonVaultBiometricPromptActivity.java com/ionicframework/IdentityVault/VaultPlugin.java com/ionicframework/auth/IdentityVault.java com/ionicframework/auth/IonicCombinedVault.java com/ionicframework/auth/IonicKeychainAuthenticatedStorage.java com/salesforce/marketingcloud/MCLogListe
4	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	

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ner.java com/salesforce/marketingcloud/cordova/MCSdkConfig.java com/salesforce/marketingcloud/g.java com/salesforce/marketingcloud/sfmcsdk/components/encryption/Encryptor.java com/salesforce/marketingcloud/sfmcsdk/components/encryption/KeyStoreWrapper.java com/salesforce/marketingcloud/sfmcsdk/components/encryption/SalesforceKeyGenerator.java com/salesforce/marketingcloud/sfmcsdk/components/logging/LogListener.java com/salesforce/marketingcloud/sfmcsdk/components/logging/Logger.java com/salesforce/marketingcloud/tozny/AesCbcWithIntegrity.java com/verint/xm/cordova/plugin/VerintXM.java com/verint/xm/sdk/common/Logging.java com/verint/xm/sdk/common/configuration/ConfigurationLoader.java io/sqlc/SQLitePlugin.java net/gotev/cookiestore/SharedPreferencesCookieStore.java net/gotev/cookiestore/WebKitSyncCookieManager.java net/sqlcipher/AbstractCursor.java net/sqlcipher/BulkCursorToCursorAdaptor.java net/sqlcipher/DatabaseUtils.java net/sqlcipher/DefaultDatabaseErrorHandler.java net/sqlcipher/database/SQLiteContentHelper.java net/sqlcipher/database/SQLiteDatabase.java net/sqlcipher/database/SQLiteDebug.java net/sqlcipher/database/SQLiteOpenHelper.java net/sqlcipher/database/SQLiteQueryBuilder.j

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ava net/sqlcipher/database/SqliteWrapper.java okio/Okio.java
5	This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files.	info	OWASP MASVS: MSTG-CRYPTO-1	okio/Options.java io/sqlc/SQLiteAndroidDatabase.java net/sqlcipher/database/SupportHelper.java
6	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/salesforce/marketingcloud/sfmcsdk/components/encryption/Encryptor.java com/salesforce/marketingcloud/sfmcsdk/components/encryption/SalesforceKeyGenerator.java
7	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/capacitorjs/plugins/camera/CameraUtils.java com/getcapacitor/BridgeWebChromeClient.java
	App uses SQLite Database and			com/salesforce/marketingcloud/storage/db/a.java com/salesforce/marketingcloud/storage/db/b.java com/salesforce/marketingcloud/storage/db/c.java com/salesforce/marketingcloud/storage/db/e.java com/salesforce/marketingcloud/storage/db/f.java com/salesforce/marketingcloud/storage/db/g.java com/salesforce/marketingcloud/storage/db/h.java com/salesforce/marketingcloud/storage/db/i.java com/salesforce/marketingcloud/storage/db/j.java com/salesforce/marketingcloud/storage/db/k.java com/salesforce/marketingcloud/storage/db/l

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	.java com/salesforce/marketingcloud/storage/db/m.java com/salesforce/marketingcloud/storage/db/upgrades/a.java com/salesforce/marketingcloud/storage/db/upgrades/b.java com/salesforce/marketingcloud/storage/db/upgrades/c.java com/salesforce/marketingcloud/storage/db/upgrades/d.java com/salesforce/marketingcloud/storage/db/upgrades/e.java com/salesforce/marketingcloud/storage/db/upgrades/f.java com/salesforce/marketingcloud/storage/db/upgrades/g.java com/salesforce/marketingcloud/storage/db/upgrades/h.java com/salesforce/marketingcloud/storage/db/upgrades/i.java com/salesforce/marketingcloud/storage/db/upgrades/j.java com/verint/xm/sdk/common/eventLogging/persistence/SQLPersister.java net/sqlcipher/database/SQLiteDatabase.java
9	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/appsflyer/internal/AFa1vSDK.java com/appsflyer/internal/AFb1bSDK.java com/verint/xm/sdk/common/b.java com/verint/xm/sdk/common/configuration/a.java com/verint/xm/sdk/common/utils/UserSamplingSelection.java com/verint/xm/sdk/predictive/tracker/NotificationWorker.java com/verint/xm/sdk/predictive/tracker/services/NotificationServiceImpl.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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	com/salesforce/marketingcloud/tozny/AesCbcWithIntegrity.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/cap/browser/plugin/WebViewDialog.java com/verint/xm/sdk/common/storyEngine/webSdkInterface/WebSdkInterface.java com/verint/xm/sdk/digital/view/DigitalActivity.java com/verint/xm/sdk/predictive/tracker/app/survey/SurveyActivity.java
12	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/verint/xm/sdk/PredictiveLaunchArgumentsHelper.java
13	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/salesforce/marketingcloud/util/l.java com/verint/xm/sdk/common/utils/Util.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/appsflyer/internal/AFg1jSDK.java com/capacitorjs/plugins/camera/CameraPlugin.java com/capacitorjs/plugins/filesystem/Filesystem.java com/capacitorjs/plugins/filesystem/FilesystemPlugin.java com/getcapacitor/FileUtils.java com/getcapacitor/plugin/http/CapacitorHttpHandler.java com/getcapacitor/plugin/util/AssetUtil.java com/salesforce/marketingcloud/storage/f.java com/salesforce/marketingcloud/util/e.java io/sqlc/SQLitePlugin.java
00013	Read file and put it into a stream	file	com/appsflyer/internal/AFa1ySDK.java com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFg1jSDK.java com/capacitorjs/plugins/filesystem/Filesystem.java com/getcapacitor/AndroidProtocolHandler.java com/salesforce/marketingcloud/storage/f.java com/salesforce/marketingcloud/tozny/AesCbcWithIntegrity.java com/salesforce/marketingcloud/util/e.java com/salesforce/marketingcloud/util/f.java com/salesforce/marketingcloud/util/g.java com/verint/xm/sdk/common/network/MultipartUtility.java
00024	Write file after Base64 decoding	reflection file	com/capacitorjs/plugins/filesystem/Filesystem.java com/salesforce/marketingcloud/tozny/AesCbcWithIntegrity.java
00094	Connect to a URL and read data from it	command network	com/capacitorjs/plugins/filesystem/Filesystem.java com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java com/verint/xm/sdk/common/network/MultipartUtility.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFj1tSDK.java com/appsflyer/internal/AFj1uSDK.java com/appsflyer/internal/AFj1vSDK.java com/appsflyer/internal/AFj1xSDK.java com/getcapacitor/FileUtils.java
00036	Get resource file from res/raw directory	reflection	com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFj1tSDK.java com/appsflyer/internal/AFj1wSDK.java com/appsflyer/internal/AFj1xSDK.java com/cap/browser/plugin/CapBrowser.java com/capacitorjs/plugins/localnotifications/LocalNotificationManager.java com/capacitorjs/plugins/localnotifications/NotificationChannelManager.java com/capacitorjs/plugins/share/SharePlugin.java com/getcapacitor/AndroidProtocolHandler.java com/getcapacitor/Bridge.java com/getcapacitor/plugin/util/AssetUtil.java com/salesforce/marketingcloud/notifications/b.java com/verint/xm/sdk/common/utils/Util.java
00014	Read file into a stream and put it into a JSON object	file	com/appsflyer/internal/AFg1jSDK.java
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/AFg1jSDK.java io/sqlc/SQLitePlugin.java
00009	Put data in cursor to JSON object	file	com/salesforce/marketingcloud/storage/db/a.java com/salesforce/marketingcloud/storage/db/d.java com/salesforce/marketingcloud/storage/db/f.java com/salesforce/marketingcloud/storage/db/m.java com/salesforce/marketingcloud/storage/db/upgrades/a.java com/salesforce/marketingcloud/storage/db/upgrades/j.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/appsflyer/internal/AFc1bSDK.java com/appsflyer/internal/AFc1kSDK.java com/appsflyer/internal/AFf1tSDK.java com/cap/browser/plugin/CapBrowser.java com/cap/browser/plugin/WebViewDialog.java com/capacitorjs/plugins/applauncher/AppLauncherPlugin.java com/capacitorjs/plugins/localnotifications/LocalNotificationManager.java com/capacitorjs/plugins/localnotifications/LocalNotificationsPlugin.java com/capacitorjs/plugins/share/SharePlugin.java com/getcapacitor/Bridge.java com/ryltsov/alex/plugins/file/opener/FileOpenerPlugin.java com/salesforce/marketingcloud/notifications/b.java com/verint/xm/sdk/common/utils/Util.java nl/raphael/settings/NativeSettingsPlugin.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/cap/browser/plugin/CapBrowser.java com/capacitorjs/plugins/applauncher/AppLauncherPlugin.java nl/raphael/settings/NativeSettingsPlugin.java
00091	Retrieve data from broadcast	collection	com/appsflyer/internal/AFb1rSDK.java com/appsflyer/internal/AFc1kSDK.java com/codingsans/ionic/smsRetriever/AndroidSmsRetriever.java com/getcapacitor/Bridge.java com/ionicframework/auth/IonicNativeAuth.java com/salesforce/marketingcloud/alarms/b.java com/salesforce/marketingcloud/messages/push/a.java com/salesforce/marketingcloud/sfmcsdk/components/behaviors/BehaviorManagerImpl.java com/verint/xm/sdk/common/LaunchArgumentsHelper.java okio/Okio.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/appsflyer/internal/AFd1hSDK.java com/appsflyer/internal/AFe1lSDK.java com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/HttpRequestHandler.java com/salesforce/marketingcloud/media/q.java com/salesforce/marketingcloud/sfmcsdk/components/http/NetworkManager.java com/verint/xm/sdk/common/network/d.java com/verint/xm/sdk/common/storyEngine/tasks/HttpAsyncTask.java com/verint/xm/sdk/predictive/tracker/tasks/HttpAsyncTask.java com/verint/xm/sdk/surveymanagement/tasks/a.java
00089	Connect to a URL and receive input stream from the server	command network	com/appsflyer/internal/AFd1hSDK.java com/appsflyer/internal/AFe1lSDK.java com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java com/salesforce/marketingcloud/media/q.java com/salesforce/marketingcloud/notifications/b.java com/salesforce/marketingcloud/sfmcsdk/components/http/NetworkManager.java com/verint/xm/sdk/common/network/MultipartUtility.java com/verint/xm/sdk/common/network/b.java com/verint/xm/sdk/common/network/d.java com/verint/xm/sdk/common/storyEngine/tasks/HttpAsyncTask.java com/verint/xm/sdk/predictive/tracker/tasks/HttpAsyncTask.java com/verint/xm/sdk/predictive/tracker/tasks/a.java
00163	Create new Socket and connecting to it	socket	com/verint/xm/sdk/common/storyEngine/tasks/HttpAsyncTask.java com/verint/xm/sdk/predictive/tracker/tasks/HttpAsyncTask.java com/verint/xm/sdk/surveymanagement/tasks/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java com/salesforce/marketingcloud/notifications/b.java com/verint/xm/sdk/common/storyEngine/tasks/HttpAsyncTask.java com/verint/xm/sdk/predictive/tracker/tasks/HttpAsyncTask.java com/verint/xm/sdk/surveymanagement/tasks/a.java
00109	Connect to a URL and get the response code	network command	com/appsflyer/internal/AFd1hSDK.java com/appsflyer/internal/AFe1lSDK.java com/appsflyer/internal/AFf1kSDK.java com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/HttpRequestHandler.java com/salesforce/marketingcloud/sfmcsdk/components/http/NetworkManager.java com/verint/xm/sdk/common/network/MultipartUtility.java com/verint/xm/sdk/common/network/b.java com/verint/xm/sdk/common/network/d.java com/verint/xm/sdk/common/storyEngine/tasks/HttpAsyncTask.java com/verint/xm/sdk/predictive/tracker/tasks/HttpAsyncTask.java com/verint/xm/sdk/predictive/tracker/tasks/a.java com/verint/xm/sdk/surveymanagement/tasks/a.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1lSDK.java com/getcapacitor/FileUtils.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1lSDK.java com/appsflyer/internal/AFj1uSDK.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFb1lSDK.java com/appsflyer/internal/AFj1uSDK.java
00072	Write HTTP input stream into a file	command network file	com/getcapacitor/plugin/util/AssetUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
00108	Read the input stream from given URL	network command	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java com/verint/xm/sdk/common/network/MultipartUtility.java
00123	Save the response to JSON after connecting to the remote server	network command	com/getcapacitor/plugin/util/CapacitorHttpUrlConnection.java com/getcapacitor/plugin/util/HttpRequestHandler.java
00153	Send binary data over HTTP	http	com/getcapacitor/plugin/util/CapacitorHttpUrlConnection.java
00054	Install other APKs from file	reflection	com/capacitorjs/plugins/camera/CameraPlugin.java
00125	Check if the given file path exist	file	com/getcapacitor/Bridge.java com/verint/xm/sdk/common/LaunchArgumentsHelper.java
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFj1uSDK.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFj1uSDK.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFj1uSDK.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFj1uSDK.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/AFi1rSDK.java
00028	Read file from assets directory	file	com/getcapacitor/FileUtils.java
00016	Get location info of the device and put it to JSON object	location collection	com/salesforce/marketingcloud/messages/d.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://member-mobile-app.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/140129283294/namespaces/firebase:fetch?key=AIzaSyA1v2Bqplmlqi5xcSbj0gTGL-hRhhxqX_Y. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.INTERNET, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE
Other Common Permissions	5/44	android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, 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
gateway.foresee.com	ok	**IP:** 18.238.109.98 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
survey-stg.foresee.com	ok	No Geolocation information available.
stg-analytics.foresee.com	ok	**IP:** 3.230.28.211 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
sinapps.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.zetetic.net	ok	**IP:** 18.238.96.105 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
analytics.foresee.com	ok	**IP:** 52.202.249.233 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.bcbsm.com	ok	**IP:** 12.176.249.78 **Country:** United States of America **Region:** Michigan **City:** Detroit **Latitude:** 42.344872 **Longitude:** -83.008118 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.
github.com	ok	**IP:** 140.82.112.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.foresee.com	ok	**IP:** 23.185.0.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.792030 **Longitude:** -122.406853 **View:** Google Map
sconversions.s	ok	No Geolocation information available.
www.verint.com	ok	**IP:** 23.185.0.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.792030 **Longitude:** -122.406853 **View:** Google Map
simpression.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.
capacitorjs.com	ok	**IP:** 104.21.93.31 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sattr.s	ok	No Geolocation information available.
stg-gateway-elb.foresee.com	ok	**IP:** 3.212.86.107 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
hoover-eu.verint-api.com	ok	**IP:** 18.185.51.12 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
sars.s	ok	No Geolocation information available.
developer.foresee.com	ok	**IP:** 52.70.206.228 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
st.foresee.com	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.
cxsuites.foresee.com	ok	No Geolocation information available.
stg-cx.foresee.com	ok	No Geolocation information available.
salesforce-marketingcloud.github.io	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
scdn-stestsettings.s	ok	No Geolocation information available.
survey.foresee.com	ok	No Geolocation information available.
hoover-eu-stg.verint-api.com	ok	**IP:** 34.252.104.243 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
hoover.foresee.com	ok	**IP:** 98.85.98.71 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
app.igodigital.com	ok	**IP:** 3.218.154.34 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
aps-webhandler.appsflyer.com	ok	**IP:** 18.238.109.70 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
stg-cxsurvey.foresee.com	ok	No Geolocation information available.
cxsurvey.foresee.com	ok	No Geolocation information available.
eus.verint-app.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
cx.foresee.com	ok	**IP:** 18.238.96.31 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
slaunches.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.
services-edge.foresee.com	ok	**IP:** 54.156.68.125 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
svalidate-and-log.s	ok	No Geolocation information available.
stage.app.igodigital.com	ok	**IP:** 98.86.87.253 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
sapp.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
s.foresee.com	ok	**IP:** 18.238.96.65 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sviap.s	ok	No Geolocation information available.
member-mobile-app.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
svalidate.s	ok	No Geolocation information available.
ionic.io	ok	**IP:** 172.66.164.120 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
stg-hoover.foresee.com	ok	**IP:** 3.230.28.211 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
services-edge-stg.foresee.com	ok	**IP:** 35.175.95.150 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

EMAILS

EMAIL	FILE
name@domain.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Salesforce Marketing Cloud		https://reports.exodus-privacy.eu.org/trackers/220

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"fileprovider_authority" : "com.bcbsm.mma.fileprovider"
"firebase_database_url" : "https://member-mobile-app.firebaseio.com"
"google_api_key" : "AIzaSyA1v2Bqplmlqi5xcSbj0gTGL-hRhhxqX_Y"
"google_crash_reporting_api_key" : "AIzaSyA1v2Bqplmlqi5xcSbj0gTGL-hRhhxqX_Y"
"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
c103703e120ae8cc73c9248622f3cd1e
29200FA5-DF79-4C3F-BC0F-E2FF3CE6199A
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901

POSSIBLE SECRETS
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
F6389234-1024-481F-9173-37D9D7F5051F
849f26e2-2df6-11e4-ab12-14109fdc48df
49f946663a8deb7054212b8adda248c6
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
1eRHtJaybutdAsFp2DkfrT1FqMJlLfT7DdgCpQtTaoQWheoeFBZRqt5pgFDH7Cf

PLAYSTORE INFORMATION

Title: BCBSM

Score: 4.5421247 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.bcbsm.mmaprod

Developer Details: Blue Cross and Blue Shield of Michigan, Blue+Cross+and+Blue+Shield+of+Michigan, None, http://bcbsm.com/app, mobileapp@bcbsm.com,

Release Date: May 18, 2016 **Privacy Policy:** Privacy link

Description:

#1 Digital Tools and Commercial Health Plan for Member Satisfaction in Michigan, three out of four years. Learn more about J.D. Power awards. With convenient access to your health plan details, you're more informed when you need care. If you're a Blue Cross Blue Shield of Michigan member, you can: -- View your deductible and other plan balances -- See what services your plan covers -- Check claims and EOBs -- Check your HSA and FSA account for users that use our Health Equity partner -- Pay your plan bill for users with non-employer coverage -- Find doctors and hospitals in your network -- Select and view your Primary Care Physician -- Get access to care including our 24-hour nurse line and telehealth -- Have your virtual ID card handy -- Compare quality ratings for doctors and procedure costs -- Research drug prices and coverage requirements -- Contact customer support -- Take your health assessment and other wellness services -- Use our Virtual Assistant to answer questions 24/7 -- Keep your secure account info updated. -- Use biometric login for faster login The app supports most of our plans, but not all. If you're one of these members, the app won't work for you: -- FEP members with a PPO plan -- MESSA members -- Blue Cross Complete (Medicaid) members Here's an overview of the permissions associated with our app and why they are needed: Identity Google Play™ services needs this in order to send you push notifications. BCBSM won't use anything related to your identity that isn't associated with your account with us. Wi-Fi connection This access allows the BCBSM app to check for an active internet connection, which allows the app to function

correctly. Photos and other media We use this access to deliver PDFs to you and to display your virtual ID card. BCBSM will not access or use your pictures or saved files for any other reason. Questions about the app? Please visit bcbsm.com/app © 1996-2025 Blue Cross Blue Shield of Michigan and Blue Care Network are nonprofit corporations and independent licensees of the Blue Cross and Blue Shield Association. We provide health insurance in Michigan.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 20:07:44	Generating Hashes	OK
2025-08-29 20:07:44	Extracting APK	OK
2025-08-29 20:07:44	Unzipping	OK
2025-08-29 20:07:45	Parsing APK with androguard	OK
2025-08-29 20:07:45	Extracting APK features using aapt/aapt2	OK
2025-08-29 20:07:45	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 20:07:47	Parsing AndroidManifest.xml	OK
2025-08-29 20:07:47	Extracting Manifest Data	OK

2025-08-29 20:07:47	Manifest Analysis Started	OK
2025-08-29 20:07:47	Reading Network Security config from network_security_config.xml	OK
2025-08-29 20:07:47	Parsing Network Security config	OK
2025-08-29 20:07:47	Performing Static Analysis on: BCBSM (com.bcbsm.mmaprod)	OK
2025-08-29 20:07:48	Fetching Details from Play Store: com.bcbsm.mmaprod	OK
2025-08-29 20:07:48	Checking for Malware Permissions	OK
2025-08-29 20:07:48	Fetching icon path	OK
2025-08-29 20:07:48	Library Binary Analysis Started	OK
2025-08-29 20:07:48	Reading Code Signing Certificate	OK
2025-08-29 20:07:49	Running APKiD 2.1.5	OK
2025-08-29 20:07:52	Detecting Trackers	OK

2025-08-29 20:07:54	Decompiling APK to Java with JADX	OK
2025-08-29 20:08:02	Converting DEX to Smali	OK
2025-08-29 20:08:02	Code Analysis Started on - java_source	OK
2025-08-29 20:08:03	Android SBOM Analysis Completed	OK
2025-08-29 20:08:07	Android SAST Completed	OK
2025-08-29 20:08:07	Android API Analysis Started	OK
2025-08-29 20:08:11	Android API Analysis Completed	OK
2025-08-29 20:08:11	Android Permission Mapping Started	OK
2025-08-29 20:08:15	Android Permission Mapping Completed	OK
2025-08-29 20:08:15	Android Behaviour Analysis Started	OK
2025-08-29 20:08:19	Android Behaviour Analysis Completed	OK

2025-08-29 20:08:19	Extracting Emails and URLs from Source Code	OK
2025-08-29 20:08:21	Email and URL Extraction Completed	OK
2025-08-29 20:08:21	Extracting String data from APK	OK
2025-08-29 20:08:21	Extracting String data from Code	OK
2025-08-29 20:08:21	Extracting String values and entropies from Code	OK
2025-08-29 20:08:23	Performing Malware check on extracted domains	OK
2025-08-29 20:08:30	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.