ANDROID STATIC ANALYSIS REPORT

mybyram (1.2.6)

File Name:	com.byram.mybyram_100421.apk
Package Name:	com.byram.mybyram
Scan Date:	Aug. 29, 2025, 8:38 p.m.
App Security Score:	58/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	14	2	3	1

FILE INFORMATION

File Name: com.byram.mybyram_100421.apk
Size: 22.5MB
MD5: 5da0325fd667b7eafdf8e70ebdc9b41b
SHA1: fa2d8c5617280b93ab5f937e7d4936d86c4a7f47
SHA256: b21af40b0047278f355a91894d94df3aed159fd81579d1180561a8cb065281c5

APP INFORMATION

App Name: mybyram
Package Name: com.byram.mybyram
Main Activity: com.tns.NativeScriptActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 1.2.6

Android Version Code: 100421

APP COMPONENTS

Activities: 4
Services: 8
Receivers: 5
Providers: 5
Exported Activities: 0
Exported Services: 0
Exported Receivers: 3
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: 2021-04-15 16:41:49+00:00
Valid To: 2051-04-15 16:41:49+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xb4d47da683be99c5a12d623de725608df87bcce1
Hash Algorithm: sha256
md5: 6fbd171cafc08cf802e86d0b9608e043
sha1: 52fe9e8a65c0bbdbb20331fb2f324bcd9302f577
sha256: 6bef6e7ebcac181ce5ed1f20b05c3d7fb95db34ed8772c145ab0abc8a2c65958
sha512: d584ccbd93873f626b6e07bd8d15f051527279f8654167549fcd0643891399fce58714a8514abe804872fe836d2697c3841f0d75308295c5eea3f3661baac98f
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 09610a7af967cd6e6b6c8d013ea3f878da352157f7aeff23f775100e260fabb2
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

PERMISSION	STATUS	INFO	DESCRIPTION
com.byram.mybyram.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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.
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.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>5da0325fd667b7eafdf8e70ebdc9b41b.apk</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>possible VM check</td></tr></table></td></tr>
</table>

<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
possible Build.SERIAL check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
<tr><td>classes2.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
network operator name check
device ID check
possible ro.secure check
possible VM 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>

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: **4** | 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	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	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
4	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.
5	Broadcast Receiver (org.nativescript.firebase.messaging.FirebaseMessaging$FirebaseMessagingReceiver) 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: **8** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/GeneratedAppGlideModuleImpl.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.java 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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				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/ResourceUriLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/DefaultOnHeaderDecodedListener.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java 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

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/gif/StreamGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SingletonConnectivityReceiver.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 com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/caverock/androidsvg/CSSParser.java com/caverock/androidsvg/SVG.java com/caverock/androidsvg/SVGAndroidRenderer.java com/caverock/androidsvg/SVGImageView.java com/caverock/androidsvg/SVGParser.java com/caverock/androidsvg/SimpleAssetResolver.java com/github/barteksc/pdfviewer/PDFView.java com/github/barteksc/pdfviewer/RenderingHandler.java com/github/barteksc/pdfviewer/link/DefaultLinkHandler.java com/nativescript/text/Font.java com/rudderstack/android/repository/EntityContentProvider.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/rudderstack/android/ruddermetricsreporterandroid/internal/DebugLogger.java com/rudderstack/android/ruddermetricsreporterandroid/internal/error/ExceptionHandler.java com/rudderstack/android/sdk/core/RudderLogger.java com/shockwave/pdfium/PdfiumCore.java com/telerik/widget/primitives/panels/RadScrollView.java com/tns/AndroidJsV8Inspector.java com/tns/AppConfig.java com/tns/AssetExtractor.java com/tns/DexFactory.java com/tns/LogcatLogger.java com/tns/ManualInstrumentation.java com/tns/NativeScriptUncaughtExceptionHandler.java com/tns/Runtime.java com/tns/RuntimeHelper.java com/tns/bindings/Dump.java com/tns/bindings/ProxyGenerator.java io/sentry/SystemOutLogger.java io/sentry/android/core/AndroidLogger.java io/sentry/transport/StdoutTransport.java jp/co/cyberagent/android/gpuimage/GLTextureView.java jp/co/cyberagent/android/gpuimage/PixelBuffer.java jp/co/cyberagent/android/gpuimage/util/OpenGlUtils.java net/gotev/uploadservice/logger/DefaultLoggerDelegate.java net/sqlcipher/AbstractCursor.java net/sqlcipher/BulkCursorToCursorAdaptor.java net/sqlcipher/DatabaseUtils.java net/sqlcipher/DefaultDatabaseErrorHandler.java net/sqlcipher/database/SQLiteCompiledSql.ja

NO	ISSUE	SEVERITY	STANDARDS	FILES
				va net/sqlcipher/database/SQLiteContentHelper.java net/sqlcipher/database/SQLiteDatabase.java net/sqlcipher/database/SQLiteDebug.java net/sqlcipher/database/SQLiteOpenHelper.java net/sqlcipher/database/SQLiteProgram.java net/sqlcipher/database/SQLiteQuery.java net/sqlcipher/database/SQLiteQueryBuilder.java net/sqlcipher/database/SqliteWrapper.java org/nativescript/Process.java org/nativescript/widgets/Async.java org/nativescript/widgets/BoxShadowDrawable.java org/nativescript/widgets/CommonLayoutParams.java org/nativescript/widgets/FileHelper.java org/nativescript/widgets/GridLayout.java org/nativescript/widgets/StackLayout.java org/nativescript/widgets/Utils.java org/nativescript/widgets/image/AsyncTask.java org/nativescript/widgets/image/Cache.java org/nativescript/widgets/image/Fetcher.java org/nativescript/widgets/image/Worker.java org/ow2/asmdex/lowLevelUtils/BasicDexFileReader.java org/ow2/asmdex/lowLevelUtils/DalvikValueReader.java org/ow2/asmdex/lowLevelUtils/DexFileReader.java org/ow2/asmdex/util/AsmDexifierApplicationVisitor.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/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/rudderstack/android/ruddermetricsreporterandroid/LibraryMetadata.java com/rudderstack/android/ruddermetricsreporterandroid/internal/DefaultUploadMediator.java com/rudderstack/android/ruddermetricsreporterandroid/internal/error/ExceptionHandler.java com/rudderstack/android/sdk/core/ReportManager.java com/rudderstack/android/sdk/core/RudderFlushWorkManager.java com/rudderstack/android/sdk/core/RudderNetworkManager.java com/rudderstack/android/sdk/core/RudderPreferenceManager.java com/rudderstack/android/sdk/core/RudderTraits.java com/tns/AppConfig.java fi/iki/elonen/NanoWSD.java io/sentry/Baggage.java io/sentry/RequestDetailsResolver.java io/sentry/TraceContext.java io/sentry/protocol/User.java net/gotev/uploadservice/extensions/ContextExtensionsKt.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	fi/iki/elonen/NanoWSD.java io/sentry/util/StringUtils.java org/nativescript/winter_cg/Crypto.java org/ow2/asmdex/ApplicationWriter.java
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	fi/iki/elonen/NanoHTTPD.java
5	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	fi/iki/elonen/NanoHTTPD.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	fi/iki/elonen/NanoHTTPD.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	io/sentry/android/core/DefaultAndroidEventProcessor.java jp/co/cyberagent/android/gpuimage/GPUImage.java jp/co/cyberagent/android/gpuimage/GPUImageView.java org/nativescript/widgets/FileHelper.java org/nativescript/widgets/image/Cache.java

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	com/rudderstack/android/repository/Dao.java com/rudderstack/android/sdk/core/DBPersistentManager.java com/rudderstack/android/sdk/core/persistence/DefaultPersistence.java com/rudderstack/android/sdk/core/persistence/DefaultPersistenceProvider.java com/rudderstack/android/sdk/core/persistence/EncryptedPersistence.java net/sqlcipher/DatabaseUtils.java net/sqlcipher/database/SQLiteDatabase.java
9	This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files.	info	OWASP MASVS: MSTG-CRYPTO-1	net/sqlcipher/database/SupportHelper.java
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/rudderstack/android/ruddermetricsreporterandroid/internal/error/RootDetector.java io/sentry/android/core/DefaultAndroidEventProcessor.java io/sentry/android/core/internal/util/RootChecker.java
11	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/RootChecker.java
12	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	org/nativescript/widgets/image/Cache.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/github/triniwiz/imagecacheit/ImageCache.java com/github/triniwiz/imagecacheit/ImageView.java com/nativescript/text/Font.java com/rudderstack/android/sdk/core/persistence/DefaultPersistenceProvider.java com/tns/AndroidJsV8Inspector.java com/tns/DexFactory.java com/tns/FileSystem.java com/tns/Module.java com/tns/Runtime.java com/tns/RuntimeHelper.java com/tns/bindings/ProxyGenerator.java fi/iki/elonen/NanoHTTPD.java io/sentry/DirectoryProcessor.java io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/SentryOptions.java io/sentry/android/core/AndroidOptionsInitializer.java io/sentry/android/core/DefaultAndroidEventProcessor.java io/sentry/android/core/cache/AndroidEnvelopeCache.java io/sentry/cache/CacheStrategy.java io/sentry/cache/EnvelopeCache.java io/sentry/instrumentation/file/FileIOSpanManager.java jp/co/cyberagent/android/gpuimage/GPUImage.java net/gotev/uploadservice/schemehandlers/FileSchemeHandler.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/resource/bitmap/ImageReader.java com/rudderstack/android/ruddermetricsreporterandroid/internal/error/RootDetector.java com/rudderstack/android/sdk/core/RudderFlushWorkManager.java com/rudderstack/android/sdk/core/RudderServerConfigManager.java com/tns/DefaultExtractPolicy.java com/tns/DexFactory.java com/tns/FileSystem.java io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/SentryEnvelopeItem.java io/sentry/cache/CacheStrategy.java io/sentry/cache/EnvelopeCache.java io/sentry/config/FilesystemPropertiesLoader.java io/sentry/instrumentation/file/FileInputStreamInitData.java io/sentry/instrumentation/file/SentryFileInputStream.java net/gotev/uploadservice/schemehandlers/FileSchemeHandler.java okio/Okio__JvmOkioKt.java org/nativescript/widgets/Async.java org/nativescript/widgets/FileHelper.java org/nativescript/widgets/image/DiskLruCache.java org/nativescript/widgets/image/Fetcher.java org/ow2/asmdex/ApplicationReader.java
00091	Retrieve data from broadcast	collection	org/nativescript/firebase/messaging/FirebaseMessaging.java
00096	Connect to a URL and set request method	command network	com/rudderstack/android/sdk/core/RudderNetworkManager.java com/rudderstack/web/internal/WebServiceImpl.java io/sentry/transport/HttpConnection.java net/gotev/uploadservice/network/hurl/HurlStackRequest.java org/nativescript/widgets/Async.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/rudderstack/android/sdk/core/RudderNetworkManager.java com/rudderstack/web/internal/WebServiceImpl.java io/sentry/transport/HttpConnection.java net/gotev/uploadservice/network/hurl/HurlStackRequest.java org/nativescript/widgets/Async.java org/nativescript/widgets/image/Fetcher.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/rudderstack/android/sdk/core/RudderNetworkManager.java com/rudderstack/web/internal/WebServiceImpl.java io/sentry/transport/HttpConnection.java org/nativescript/widgets/Async.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java com/rudderstack/android/sdk/core/RudderNetworkManager.java com/rudderstack/web/internal/WebServiceImpl.java io/sentry/transport/HttpConnection.java net/gotev/uploadservice/network/hurl/HurlStackRequest.java org/nativescript/widgets/Async.java
00039	Start a web server	control network	fi/iki/elonen/NanoHTTPD.java
00189	Get the content of a SMS message	sms	net/gotev/uploadservice/schemehandlers/ContentResolverSchemeHandler.java
00188	Get the address of a SMS message	sms	net/gotev/uploadservice/schemehandlers/ContentResolverSchemeHandler.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	net/gotev/uploadservice/schemehandlers/ContentResolverSchemeHandler.java org/nativescript/widgets/image/Fetcher.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/rudderstack/android/repository/EntityContentProvider.java net/gotev/uploadservice/schemehandlers/ContentResolverSchemeHandler.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	net/gotev/uploadservice/schemehandlers/ContentResolverSchemeHandler.java org/nativescript/widgets/FileHelper.java
00200	Query data from the contact list	collection contact	net/gotev/uploadservice/schemehandlers/ContentResolverSchemeHandler.java
00201	Query data from the call log	collection calllog	net/gotev/uploadservice/schemehandlers/ContentResolverSchemeHandler.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/rudderstack/android/repository/EntityContentProvider.java net/gotev/uploadservice/schemehandlers/ContentResolverSchemeHandler.java
00003	Put the compressed bitmap data into JSON object	camera	com/github/triniwiz/imagecacheit/ImageView.java
00005	Get absolute path of file and put it to JSON object	file	com/github/triniwiz/imagecacheit/ImageView.java com/nativescript/text/Font.java com/tns/AndroidJsV8Inspector.java com/tns/Module.java
00004	Get filename and put it to JSON object	file collection	com/github/triniwiz/imagecacheit/ImageView.java com/tns/Module.java
00036	Get resource file from res/raw directory	reflection	com/github/triniwiz/imagecacheit/ImageView.java com/rudderstack/android/repository/EntityContentProvider.java org/nativescript/widgets/Async.java org/nativescript/widgets/Utils.java org/nativescript/widgets/image/Fetcher.java

RULE ID	BEHAVIOUR	LABEL	FILES
00012	Read data and put it into a buffer stream	file	com/tns/FileSystem.java io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/SentryEnvelopeItem.java io/sentry/cache/CacheStrategy.java io/sentry/cache/EnvelopeCache.java io/sentry/config/FilesystemPropertiesLoader.java org/nativescript/widgets/Async.java org/nativescript/widgets/image/DiskLruCache.java org/nativescript/widgets/image/Fetcher.java
00094	Connect to a URL and read data from it	command network	com/rudderstack/android/sdk/core/RudderNetworkManager.java org/nativescript/widgets/Async.java org/nativescript/widgets/image/Fetcher.java
00108	Read the input stream from given URL	network command	com/rudderstack/android/sdk/core/RudderNetworkManager.java org/nativescript/widgets/Async.java org/nativescript/widgets/image/Fetcher.java
00028	Read file from assets directory	file	com/caverock/androidsvg/SimpleAssetResolver.java
00072	Write HTTP input stream into a file	command network file	org/nativescript/widgets/Async.java
00024	Write file after Base64 decoding	reflection file	org/nativescript/widgets/Async.java
00068	Executes the specified string Linux command	control	com/tns/Util.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/github/barteksc/pdfviewer/link/DefaultLinkHandler.java

RULE ID	BEHAVIOUR	LABEL	FILES
00163	Create new Socket and connecting to it	socket	com/rudderstack/android/sdk/core/RudderNetworkManager.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/96794398918/namespaces/firebase:fetch?key=AIzaSyCbB3o1cDAuPGAEHFjttPu9R97Qe6B_50I. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.CAMERA, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE, android.permission.READ_PHONE_STATE
Other Common Permissions	3/44	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
docs.bugsnag.com	ok	**IP:** 18.155.173.77 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.zetetic.net	ok	**IP:** 18.238.96.111 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
stackoverflow.com	ok	**IP:** 104.18.32.7 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
hosted.rudderlabs.com	ok	**IP:** 34.196.19.127 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.rudderlabs.com	ok	**IP:** 18.238.96.121 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

TRACKER	CATEGORIES	URL
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AIzaSyCbB3o1cDAuPGAEHFjttPu9R97Qe6B_50I"
"google_crash_reporting_api_key" : "AIzaSyCbB3o1cDAuPGAEHFjttPu9R97Qe6B_50I"
"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

PLAYSTORE INFORMATION

Title: mybyram: Medical Supply Orders

Score: 4.7807627 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.byram.mybyram

Developer Details: Byram Healthcare Centers, Inc., Byram+Healthcare+Centers,+Inc., None, https://www.mybyramhealthcare.com/, mybyramapp@byramhealthcare.com,

Release Date: Apr 16, 2021 **Privacy Policy:** Privacy link

Description:

Accessing your Byram Healthcare account is quick and secure. You can use facial recognition or your fingerprint for added convenience. Here's what you can do once you're in: Reorder Easily: Quickly reorder products you've ordered before with just a few clicks. Flexible Supply Options: Order supplies for 30 days or 90 days*, depending on your needs. Browse & Add Products: Explore our product catalog and easily add new items* to your order. Order Tracking: Track the status of your order, including shipping details, so you know when to expect your supplies. Access Order History: View your previous orders from the past year, making it easy to track your history. Secure Payments: Make payments securely using your credit card, Google Pay™, or Apple Pay™. Update Account Info: Keep your account details up to date, ensuring accurate information. Manage Physician and Insurance Info: Conveniently manage your physician and insurance information in one place. Live Chat Support: Get your questions answered and receive support through our Live Chat feature. * Please note: Not all healthcare insurance plans allow new products to be ordered and/or the ordering of 90-day supplies.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 20:38:18	Generating Hashes	OK
2025-08-29 20:38:18	Extracting APK	OK
2025-08-29 20:38:18	Unzipping	OK
2025-08-29 20:38:19	Parsing APK with androguard	OK
2025-08-29 20:38:19	Extracting APK features using aapt/aapt2	OK
2025-08-29 20:38:19	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 20:38:20	Parsing AndroidManifest.xml	OK

2025-08-29 20:38:20	Extracting Manifest Data	OK
2025-08-29 20:38:20	Manifest Analysis Started	OK
2025-08-29 20:38:20	Performing Static Analysis on: mybyram (com.byram.mybyram)	OK
2025-08-29 20:38:21	Fetching Details from Play Store: com.byram.mybyram	OK
2025-08-29 20:38:22	Checking for Malware Permissions	OK
2025-08-29 20:38:22	Fetching icon path	OK
2025-08-29 20:38:22	Library Binary Analysis Started	OK
2025-08-29 20:38:22	Reading Code Signing Certificate	OK
2025-08-29 20:38:22	Running APKiD 2.1.5	OK
2025-08-29 20:38:26	Detecting Trackers	OK

2025-08-29 20:38:29	Decompiling APK to Java with JADX	OK
2025-08-29 20:38:43	Converting DEX to Smali	OK
2025-08-29 20:38:43	Code Analysis Started on - java_source	OK
2025-08-29 20:38:45	Android SBOM Analysis Completed	OK
2025-08-29 20:38:54	Android SAST Completed	OK
2025-08-29 20:38:54	Android API Analysis Started	OK
2025-08-29 20:39:01	Android API Analysis Completed	OK
2025-08-29 20:39:02	Android Permission Mapping Started	OK
2025-08-29 20:39:09	Android Permission Mapping Completed	OK
2025-08-29 20:39:09	Android Behaviour Analysis Started	OK

2025-08-29 20:39:17	Android Behaviour Analysis Completed	OK
2025-08-29 20:39:17	Extracting Emails and URLs from Source Code	OK
2025-08-29 20:39:19	Email and URL Extraction Completed	OK
2025-08-29 20:39:19	Extracting String data from APK	OK
2025-08-29 20:39:19	Extracting String data from Code	OK
2025-08-29 20:39:19	Extracting String values and entropies from Code	OK
2025-08-29 20:39:21	Performing Malware check on extracted domains	OK
2025-08-29 20:39:22	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.