ANDROID STATIC ANALYSIS REPORT

MyBenefits2GO (1.1.0)

File Name:	com.usi.ebmobile_47414.apk
Package Name:	com.usi.ebmobile
Scan Date:	Sept. 1, 2025, 11:07 a.m.
App Security Score:	50/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	25	2	1	1

FILE INFORMATION

File Name: com.usi.ebmobile_47414.apk
Size: 22.18MB
MD5: b05e0a10bc1d69eac37131690536cef3
SHA1: 54a0dc4c1c3c99d8b49f155e0468679bb0cc1498
SHA256: 23372e1246a2d3f368c7e7628460485bd8949af5262fcd4bdaa9404401d7e6e6

APP INFORMATION

App Name: MyBenefits2GO
Package Name: com.usi.ebmobile
Main Activity: com.usi.ebmobile.ui.SplashActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 1.1.0

Android Version Code: 47414

APP COMPONENTS

Activities: 18
Services: 11
Receivers: 14
Providers: 3
Exported Activities: 7
Exported Services: 1
Exported Receivers: 7
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-05-13 22:45:03+00:00
Valid To: 2051-05-13 22:45:03+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xc6028306cc6cec2e9ab6e9e0188e0333c021e2ed
Hash Algorithm: sha256
md5: 7300fbf8816d7c7fe8536a2ab2077126
sha1: f835b9953e677ba2f24f2356d436a5c2011577e9
sha256: ad4e6f4f9e619f770be38413c38b8241765d167487609a921d2b370a427d9c11
sha512: 2bf04b2027f8e7a5c679b14f407bb2a8598c3b2b866c2d8c098e1522cf6ca5f90ddc152de286e7061f029e925dde484dae36c917c75d4121ec9f36108518e9d1
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 96153a0c0bb77b4d1c247f10bc1aa8a14f8e9706f5bc6744766bd288ee06879b
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_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
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.
com.usi.ebmobile.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.

PERMISSION	STATUS	INFO	DESCRIPTION
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.usi.ebmobile.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>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
network operator name check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</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: **0** | WARNING: **17** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Activity (com.usi.ebmobile.ui.OutageActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
3	Activity (com.usi.ebmobile.ui.ErrorActivity) 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.usi.ebmobile.ui.InvalidAccessCodeLaunchActivity) 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.usi.ebmobile.ui.FatalErrorActivity) 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	Broadcast Receiver (com.onesignal.FCMBroadcastReceiver) 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.
7	Activity (com.onesignal.NotificationOpenedActivityHMS) 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.
8	Broadcast Receiver (com.onesignal.NotificationDismissReceiver) is not Protected. [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.
9	Broadcast Receiver (com.onesignal.BootUpReceiver) is not Protected. [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.
10	Broadcast Receiver (com.onesignal.UpgradeReceiver) is not Protected. [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.
11	Activity (com.onesignal.NotificationOpenedReceiver) 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
12	Activity (com.onesignal.NotificationOpenedReceiverAndroid22AndOlder) 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.
13	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.
14	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.
15	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
16	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.
17	High Intent Priority (999) - {1} Hit(s) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

CODE ANALYSIS

HIGH: **1** | WARNING: **6** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				/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
				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

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/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/microsoft/appcenter/AbstractAppCenterService.java com/microsoft/appcenter/AppCenter.java com/microsoft/appcenter/Constants.java com/microsoft/appcenter/CustomProperties.java com/microsoft/appcenter/Flags.java com/microsoft/appcenter/ServiceInstrumentationUtils.java com/microsoft/appcenter/UncaughtExceptionHandler.java com/microsoft/appcenter/analytics/Analytics.java com/microsoft/appcenter/analytics/AnalyticsTransmissionTarget.java com/microsoft/appcenter/analytics/AuthenticationProvider.java com/microsoft/appcenter/analytics/EventProperties.java com/microsoft/appcenter/analytics/channel/AnalyticsValidator.java com/microsoft/appcenter/analytics/channel/SessionTracker.java com/microsoft/appcenter/analytics/ingestion/models/EventLog.java com/microsoft/appcenter/analytics/ingestion/models/json/EventLogFactory.java com/microsoft/appcenter/channel/DefaultChannel.java com/microsoft/appcenter/channel/OneCollectorChannelListener.java com/microsoft/appcenter/crashes/Crashes.java com/microsoft/appcenter/crashes/WrapperSdkExceptionManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/microsoft/appcenter/crashes/ingestion/models/AbstractErrorLog.java com/microsoft/appcenter/crashes/ingestion/models/ErrorAttachmentLog.java com/microsoft/appcenter/crashes/ingestion/models/HandledErrorLog.java com/microsoft/appcenter/crashes/ingestion/models/ManagedErrorLog.java com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java com/microsoft/appcenter/http/AbstractAppCallTemplate.java com/microsoft/appcenter/http/DefaultHttpClient.java com/microsoft/appcenter/http/DefaultHttpClientCallTask.java com/microsoft/appcenter/http/HttpClientNetworkStateHandler.java com/microsoft/appcenter/http/HttpClientRetryer.java com/microsoft/appcenter/ingestion/OneCollectorIngestion.java com/microsoft/appcenter/ingestion/models/AbstractLog.java com/microsoft/appcenter/ingestion/models/one/CommonSchemaDataUtils.java com/microsoft/appcenter/ingestion/models/one/CommonSchemaLog.java com/microsoft/appcenter/ingestion/models/one/PartAUtils.java com/microsoft/appcenter/persistence/DatabasePersistence.java com/microsoft/appcenter/utils/AppCenterLog.java com/microsoft/appcenter/utils/AsyncTaskUtils.java com/microsoft/appcenter/utils/DeviceInfoHelper.java com/microsoft/appcenter/utils/IdHelper.java com/microsoft/appcenter/utils/NetworkSta

NO	ISSUE	SEVERITY	STANDARDS	FILES
				teHelper.java com/microsoft/appcenter/utils/context/SessionContext.java com/microsoft/appcenter/utils/context/UserIdContext.java com/microsoft/appcenter/utils/crypto/CryptoUtils.java com/microsoft/appcenter/utils/storage/DatabaseManager.java com/microsoft/appcenter/utils/storage/FileManager.java com/onesignal/AndroidSupportV4Compat.java com/onesignal/JobIntentService.java com/onesignal/OneSignal.java com/onesignal/shortcutbadger/ShortcutBadger.java com/rajat/pdfviewer/PdfDownloader$download$2.java com/rajat/pdfviewer/PdfRendererCore$writeBitmapToCache$1.java com/rajat/pdfviewer/PdfRendererCore.java com/rajat/pdfviewer/PdfViewerActivity.java com/usi/ebmobile/adapter/DeletePlanDetailsAdapter.java com/usi/ebmobile/adapter/MessageAdapter.java com/usi/ebmobile/api/ApiApp.java com/usi/ebmobile/bl/AccessCodeManager.java com/usi/ebmobile/bl/UserDeviceManager.java com/usi/ebmobile/db/AccessCodeRepository.java com/usi/ebmobile/db/DatabaseHelper.java com/usi/ebmobile/db/FavoriteRepository.java com/usi/ebmobile/db/IDCardRepository.java com/usi/ebmobile/db/MessageRepository.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/usi/ebmobile/db/UserRepository.java com/usi/ebmobile/ui/RegistrationActivity$doRegister$1.java com/usi/ebmobile/ui/RegistrationActivity.java com/usi/ebmobile/util/EBMobileLifecycleObserver.java com/usi/ebmobile/util/ExceptionHandler.java com/usi/ebmobile/util/ScaleImage.java
2	Files may contain hardcoded sensitive information like usernames,	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering	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/microsoft/appcenter/AppCenter.java com/microsoft/appcenter/Constants.java com/microsoft/appcenter/channel/DefaultChannel.java com/microsoft/appcenter/http/DefaultHttpClient.java com/microsoft/appcenter/ingestion/OneCollectorIngestion.java com/microsoft/appcenter/ingestion/models/WrapperSdk.java com/microsoft/appcenter/ingestion/models/one/CommonSchemaLog.java com/microsoft/appcenter/persistence/DatabasePersistence.java com/microsoft/appcenter/utils/context/SessionContext.java com/microsoft/appcenter/utils/storage/DatabaseManager.java com/onesignal/FCMBroadcastReceiver.java com/onesignal/NotificationBundleProcesso

NO	ISSUE	SEVERITY	STANDARDS	FILES
	passwords, keys etc.		OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	r.java com/onesignal/OSEmailSubscriptionState.java com/onesignal/OSInAppMessageController.java com/onesignal/OSInAppMessageLocationPrompt.java com/onesignal/OSInAppMessagePrompt.java com/onesignal/OSInAppMessagePushPrompt.java com/onesignal/OSInAppMessageRepository.java com/onesignal/OSNotification.java com/onesignal/OSNotificationController.java com/onesignal/OSPermissionState.java com/onesignal/OSSMSSubscriptionState.java com/onesignal/OSSubscriptionState.java com/onesignal/OneSignalHmsEventBridge.java com/onesignal/OneSignalNotificationManager.java com/onesignal/OneSignalRemoteParams.java com/onesignal/UserState.java com/onesignal/UserStateSynchronizer.java com/onesignal/WebViewManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/microsoft/appcenter/persistence/DatabasePersistence.java com/microsoft/appcenter/utils/storage/DatabaseManager.java com/onesignal/OneSignalDbHelper.java com/onesignal/outcomes/data/OSOutcomeTableProvider.java com/usi/ebmobile/db/AccessCodeRepository.java com/usi/ebmobile/db/DatabaseHelper.java com/usi/ebmobile/db/FavoriteRepository.java com/usi/ebmobile/db/IDCardRepository.java com/usi/ebmobile/db/MessageRepository.java com/usi/ebmobile/db/UserRepository.java
4	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/rajat/pdfviewer/PdfViewerActivity.java com/rajat/pdfviewer/util/FileUtils.java com/usi/ebmobile/util/FileHelper.java
5	This App uses SQL Cipher. Ensure that secrets are not hardcoded in code.	info	OWASP MASVS: MSTG-CRYPTO-1	com/microsoft/appcenter/utils/storage/DatabaseManager.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/usi/ebmobile/api/ApiApp.java com/usi/ebmobile/api/ApiBase.java
7	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/onesignal/WebViewManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/onesignal/WebViewManager.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/microsoft/appcenter/http/HttpClientRetryer.java com/onesignal/OSUtils.java
10	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/rajat/pdfviewer/PdfDownloader$download$2.java com/rajat/pdfviewer/util/FileUtils.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/onesignal/NavigateToAndroidSettingsForLocation.java com/onesignal/OSUtils.java com/onesignal/shortcutbadger/impl/OPPOHomeBader.java com/onesignal/shortcutbadger/impl/SonyHomeBadger.java com/rajat/pdfviewer/PdfViewerActivity.java com/usi/ebmobile/adapter/DeleteHomeAdapter.java com/usi/ebmobile/adapter/DeletePlanDetailDocAdapter.java com/usi/ebmobile/adapter/DeletePlanDetailsAdapter.java com/usi/ebmobile/adapter/FavoriteAdapter.java com/usi/ebmobile/adapter/ResourceDocAdapter.java com/usi/ebmobile/adapter/ResourceItemAdapter.java
00022	Open a file from given absolute path of the file	file	com/microsoft/appcenter/crashes/Crashes.java com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java com/microsoft/appcenter/utils/storage/FileManager.java com/rajat/pdfviewer/PdfDownloader$download$2.java com/rajat/pdfviewer/PdfDownloader.java com/rajat/pdfviewer/util/CacheManager.java com/usi/ebmobile/util/ImageHelper.java
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/microsoft/appcenter/utils/storage/FileManager.java com/rajat/pdfviewer/PdfViewerActivity.java com/usi/ebmobile/util/ImageHelper.java okio/Okio.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/onesignal/NavigateToAndroidSettingsForLocation.java com/onesignal/OSUtils.java com/usi/ebmobile/adapter/DeletePlanDetailsAdapter.java com/usi/ebmobile/adapter/FavoriteAdapter.java com/usi/ebmobile/adapter/ResourceItemAdapter.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/onesignal/NavigateToAndroidSettingsForLocation.java com/onesignal/OSUtils.java com/onesignal/shortcutbadger/impl/EverythingMeHomeBadger.java com/onesignal/shortcutbadger/impl/HuaweiHomeBadger.java com/onesignal/shortcutbadger/impl/NovaHomeBadger.java com/onesignal/shortcutbadger/impl/OPPOHomeBader.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java com/onesignal/shortcutbadger/impl/SonyHomeBadger.java
00091	Retrieve data from broadcast	collection	com/onesignal/BundleCompatBundle.java com/onesignal/FCMBroadcastReceiver.java com/onesignal/OSNotificationFormatHelper.java com/onesignal/PermissionsActivity.java com/rajat/pdfviewer/PdfViewerActivity.java
00009	Put data in cursor to JSON object	file	com/onesignal/GenerateNotification.java com/onesignal/NotificationBundleProcessor.java com/onesignal/NotificationOpenedProcessor.java com/onesignal/NotificationSummaryManager.java com/onesignal/OSInAppMessageRepository.java
00202	Make a phone call	control	com/usi/ebmobile/adapter/DeletePlanDetailsAdapter.java com/usi/ebmobile/adapter/FavoriteAdapter.java com/usi/ebmobile/adapter/ResourceItemAdapter.java
00203	Put a phone number into an intent	control	com/usi/ebmobile/adapter/DeletePlanDetailsAdapter.java com/usi/ebmobile/adapter/FavoriteAdapter.java com/usi/ebmobile/adapter/ResourceItemAdapter.java
00189	Get the content of a SMS message	sms	com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00188	Get the address of a SMS message	sms	com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00191	Get messages in the SMS inbox	sms	com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00200	Query data from the contact list	collection contact	com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00187	Query a URI and check the result	collection sms calllog calendar	com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00201	Query data from the call log	collection calllog	com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00112	Get the date of the calendar event	collection calendar	com/usi/ebmobile/util/CommonMethods.java
00096	Connect to a URL and set request method	command network	com/onesignal/OneSignalRestClient.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/onesignal/OneSignalRestClient.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java com/onesignal/OneSignalRestClient.java
00177	Check if permission is granted and request it	permission	com/onesignal/AndroidSupportV4Compat.java
00092	Send broadcast	command	com/onesignal/NotificationOpenedProcessor.java

RULE ID	BEHAVIOUR	LABEL	FILES
00078	Get the network operator name	collection telephony	com/microsoft/appcenter/utils/DeviceInfoHelper.java com/onesignal/OSUtils.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java
00005	Get absolute path of file and put it to JSON object	file	com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java
00004	Get filename and put it to JSON object	file collection	com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java
00132	Query The ISO country code	telephony collection	com/microsoft/appcenter/utils/DeviceInfoHelper.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	3/44	android.permission.CALL_PHONE, com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_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
in.appcenter.ms	ok	**IP:** 4.152.45.235 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.usi.com	ok	**IP:** 104.18.38.147 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api-ebmobile.usi.com	ok	**IP:** 139.60.216.205 **Country:** United States of America **Region:** Pennsylvania **City:** Philadelphia **Latitude:** 39.869377 **Longitude:** -75.286438 **View:** Google Map
mobile.events.data.microsoft.com	ok	**IP:** 20.42.65.93 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **View:** Google Map
api.onesignal.com	ok	**IP:** 104.17.111.223 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Microsoft Visual Studio App Center Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/243

TRACKER	CATEGORIES	URL
Microsoft Visual Studio App Center Crashes	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/238
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193

HARDCODED SECRETS

POSSIBLE SECRETS
c682b8144a8dd52bc1ad63
c103703e120ae8cc73c9248622f3cd1e
f5d0fb83-af6d-4c64-a01e-81b2100ac5a3
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
2869d05c-596e-4766-ad5b-f0edf1c10dcc
5eb5a37e-b458-11e3-ac11-000c2940e62c
49f946663a8deb7054212b8adda248c6
b2f7f966-d8cc-11e4-bed1-df8f05be55ba

PLAYSTORE INFORMATION

Title: MyBenefits2GO

Score: 4.1666665 **Installs:** 10,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.usi.ebmobile

Developer Details: USI, USI, None, https://www.usi.com/contact-us/, EBSolutions@usi.com,

Release Date: Nov 8, 2021 **Privacy Policy:** Privacy link

Description:

USI MyBenefits2GO gives you access to your employer benefit information from the convenience of your mobile device. Download the app and register with the access code provided by your employer. Once signed in, your important benefit details are at your fingertips. • Access key details about your benefits • View, save and send digital copies of your insurance cards • Easily find group ID number, plan summaries and other helpful information • Contact your insurance providers with a push of a button • Get reminders for open enrollment and wellness dates

SCAN LOGS

Timestamp	Event	Error
2025-09-01 11:07:09	Generating Hashes	OK
2025-09-01 11:07:09	Extracting APK	OK
2025-09-01 11:07:09	Unzipping	OK
2025-09-01 11:07:09	Parsing APK with androguard	OK
2025-09-01 11:07:09	Extracting APK features using aapt/aapt2	OK

2025-09-01 11:07:09	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 11:07:12	Parsing AndroidManifest.xml	OK
2025-09-01 11:07:12	Extracting Manifest Data	OK
2025-09-01 11:07:12	Manifest Analysis Started	OK
2025-09-01 11:07:12	Performing Static Analysis on: MyBenefits2GO (com.usi.ebmobile)	OK
2025-09-01 11:07:13	Fetching Details from Play Store: com.usi.ebmobile	OK
2025-09-01 11:07:15	Checking for Malware Permissions	OK
2025-09-01 11:07:15	Fetching icon path	OK
2025-09-01 11:07:16	Library Binary Analysis Started	OK
2025-09-01 11:07:16	Reading Code Signing Certificate	OK
2025-09-01 11:07:16	Running APKiD 2.1.5	OK

2025-09-01 11:07:18	Detecting Trackers	OK
2025-09-01 11:07:20	Decompiling APK to Java with JADX	OK
2025-09-01 11:07:36	Converting DEX to Smali	OK
2025-09-01 11:07:36	Code Analysis Started on - java_source	OK
2025-09-01 11:07:37	Android SBOM Analysis Completed	OK
2025-09-01 11:07:42	Android SAST Completed	OK
2025-09-01 11:07:42	Android API Analysis Started	OK
2025-09-01 11:07:45	Android API Analysis Completed	OK
2025-09-01 11:07:46	Android Permission Mapping Started	OK
2025-09-01 11:07:49	Android Permission Mapping Completed	OK
2025-09-01 11:07:49	Android Behaviour Analysis Started	OK

2025-09-01 11:07:53	Android Behaviour Analysis Completed	OK
2025-09-01 11:07:53	Extracting Emails and URLs from Source Code	OK
2025-09-01 11:07:54	Email and URL Extraction Completed	OK
2025-09-01 11:07:54	Extracting String data from APK	OK
2025-09-01 11:07:55	Extracting String data from Code	OK
2025-09-01 11:07:55	Extracting String values and entropies from Code	OK
2025-09-01 11:07:57	Performing Malware check on extracted domains	OK
2025-09-01 11:07:58	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.