MOBSF

ANDROID STATIC ANALYSIS REPORT

app_icon

Amaha (InnerHour) (3.85)

File Name:	Amaha_3.85_apkcombo.com.apk
Package Name:	com.theinnerhour.b2b
Scan Date:	Dec. 3, 2023, 9:37 p.m.
App Security Score:	34/100 (HIGH RISK)
Grade:	
Trackers Detection:	7/428

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
12	15	3	2	2

FILE INFORMATION

File Name: Amaha_3.85_apkcombo.com.apk
Size: 22.54MB
MD5: 4f1ee70e900c25d0954e36b48f88472e
SHA1: e8abf47afa09141eb2c4505f48e75df722a9de5b
SHA256: 2cf3f3cfdc1b2e65b64d186f06377abcf8698cfbe2cf85fd14ee77ef0f38b409

APP INFORMATION

App Name: Amaha (InnerHour)
Package Name: com.theinnerhour.b2b
Main Activity: com.theinnerhour.b2b.components.splash.activity.SplashScreenActivity
Target SDK: 33
Min SDK: 21
Max SDK:
Android Version Name: 3.85

Android Version Code: 214

APP COMPONENTS

Activities: 154
Services: 24
Receivers: 21
Providers: 5
Exported Activities: 6
Exported Services: 2
Exported Receivers: 5
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=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-08-05 16:42:13+00:00
Valid To: 2047-08-05 16:42:13+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xbd24be643f741a309ad2e5beedf41fbe68093da1
Hash Algorithm: sha256
md5: a9f7d940d9cfb21b6c8e28bbb7f6e8ca
sha1: 3901150ea4fde3182a0bea8777e665b9e2e0a296
sha256: fe0096b1709c360df8a2409d26a5f9186ab0e041cb14fcb9403c2ff7463c1c0f
sha512: b198b0219b53e14e4462fdb63ffd4641fc7635831e5a0ac3a78a92fbec39a3ef143f43ff5e91813e1efa96f908932c6483099e847bac5b3e5088fbcd9d862b6f
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 20647dbb38168e29665685c2a444a79f2bbbd76663073b61e384b2506319ec8b
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.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.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.

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.android.alarm.permission.SET_ALARM	unknown	Unknown permission	Unknown permission from android reference
android.permission.SCHEDULE_EXACT_ALARM	normal		Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
com.android.vending.BILLING	unknown	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	unknown	Unknown permission	Unknown permission from android reference
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
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.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.

PERMISSION	STATUS	INFO	DESCRIPTION
com.theinnerhour.b2b.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.

APKID ANALYSIS

FILE	DETAILS

<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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator check
network operator name check
device ID check
ro.hardware check
ro.kernel.qemu 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>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes3.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.theinnerhour.b2b.components.splash.activity.SplashScreenActivity	Schemes: https://, http://, Hosts: www.theinnerhour.com, www.amahahealth.com, innerhour.page.link, theinnerhour.page.link, amahahealth.page.link, amaha.page.link, Path Prefixes: /appointment, /psychappointment, /sellingscreen, /article, /activity,
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.com.theinnerhour.b2b,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

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: 10 | WARNING: 5 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=21]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Broadcast Receiver (com.theinnerhour.b2b.receiver.BootReceiver) is not Protected. [android:exported=true]	high	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.
4	Broadcast Receiver (com.theinnerhour.b2b.receiver.InnerHourBroadCastReceiver) is not Protected. [android:exported=true]	high	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.
5	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	high	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 (androidx.media.session.MediaButtonReceiver) is not Protected. [android:exported=true]	high	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.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
8	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.
9	Activity (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Activity (com.google.firebase.auth.internal.RecaptchaActivity) is not Protected. [android:exported=true]	high	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
11	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.
12	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.
13	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
14	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) is not Protected. [android:exported=true]	high	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
15	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

</> CODE ANALYSIS

HIGH: **1** | WARNING: **8** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	a4/d.java com/bugsnag/android/DeliveryHeadersKt.java com/bugsnag/android/EventFilenameInfo.java com/bugsnag/android/ExceptionHandler.java com/bugsnag/android/ManifestConfigLoader.java com/bugsnag/android/SharedPrefMigrator.java com/bugsnag/android/SystemBroadcastReceiver.java com/bugsnag/android/internal/ImmutableConfig.java com/theinnerhour/b2b/components/dynamicActivities/data/NewDynamicActivityUploadModel.java com/theinnerhour/b2b/network/model/TelecommunicationsHomeworkResponseModel.java com/theinnerhour/b2b/network/model/UpcomingBooking.java com/theinnerhour/b2b/persistence/GoalsNotificationPersistence.java com/theinnerhour/b2b/persistence/GoalsPersistence.java com/theinnerhour/b2b/utils/Constants.java com/theinnerhour/b2b/utils/SessionManager.java fe/g.java h4/f.java ie/a.java ih/d.java k4/f.java k4/q.java k4/x.java ke/n.java le/f.java ne/c0.java v2/d.java wr/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				xh/e.java a0/e.java a0/f.java a0/g.java a0/h.java a0/j.java a0/k.java a0/l.java a0/n.java a1/c.java a3/q.java a5/d.java a5/i.java a8/d.java aa/j.java aa/k.java ab/g.java ad/b.java ad/i.java am/w.java b0/a.java b0/b.java b0/f.java b2/c.java b7/b.java b8/b.java b8/e.java b8/f.java b8/h.java b8/k.java b9/l.java b9/n.java bo/e.java c2/c.java c4/u.java c8/i.java ca/a.java com/airbnb/lottie/LottieAnimationView.java com/appsflyer/AFLogger.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/appsflyer/internal/AFa1cSDK.java com/appsflyer/internal/AFa1sSDK.java com/appsflyer/internal/AFb1xSDK.java com/appsflyer/internal/AFc1bSDK.java com/appsflyer/internal/AFc1cSDK.java com/appsflyer/internal/AFc1eSDK.java com/appsflyer/internal/AFc1lSDK.java com/appsflyer/internal/AFc1mSDK.java com/appsflyer/internal/AFc1uSDK.java com/appsflyer/internal/AFd1aSDK.java com/appsflyer/internal/AFd1fSDK.java com/appsflyer/internal/AFd1oSDK.java com/appsflyer/internal/AFd1rSDK.java com/appsflyer/internal/AFd1sSDK.java com/appsflyer/internal/AFd1uSDK.java com/appsflyer/internal/AFd1vSDK.java com/appsflyer/share/LinkGenerator.java com/bugsnag/android/DebugLogger.java com/bugsnag/android/ExceptionHandler.java com/bumptech/glide/Glide.java com/bumptech/glide/e.java com/bumptech/glide/f.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/canhub/cropper/CropImageActivity.java com/canhub/cropper/CropImageView.java com/canhub/cropper/CropOverlayView.java com/canhub/cropper/c.java com/davemorrissey/labs/subscaleview/SubsamplingScaleImageView.java com/davemorrissey/labs/subscaleview/decoder/SkiaPooledImageRegionDecoder.java com/github/mikephil/charting/charts/BarChart.java com/hbb20/CountryCodePicker.java com/hbb20/a.java com/tbuonomo/viewpagerdotsindicator/DotsIndicator.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/theinnerhour/b2b/MyApplication.java com/theinnerhour/b2b/activity/TemplateActivity.java com/theinnerhour/b2b/components/dynamicActivities/utils/MusicService.java com/theinnerhour/b2b/components/dynamicActivities/utils/a.java com/theinnerhour/b2b/components/pro/assessment/activity/ProInitialAssessmentActivity.java com/theinnerhour/b2b/components/recommendedActivities/activity/RecommendedActivitiesPlaybackActivity.java d2/a.java d8/c0.java d8/f.java d8/l.java d8/o.java d8/t.java d8/w.java d9/g.java defpackage/c.java defpackage/d.java df/a.java df/b.java e4/h.java e4/o.java e5/a.java e7/k.java e8/a.java e8/c.java ea/b.java f0/b.java f0/f.java f0/f0.java f0/g.java f0/n.java f0/v.java f0/y.java f1/a.java f6/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				f6/b.java f6/c.java g/j.java g/k.java g/l.java g/v.java g/w.java g/x.java g/y.java g0/a.java g2/a.java g4/d.java g4/e.java g6/r.java g6/y.java g9/a.java g9/b.java gd/c0.java gd/d.java gd/h0.java gd/p.java gd/t.java h1/a.java h5/c.java h5/g0.java h5/p.java h5/q.java h5/u.java h5/x.java h7/a.java hb/a.java hc/d.java hc/g.java hc/i.java hc/k.java hd/a.java hd/d.java hd/h.java i0/f.java i0/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				i2/d.java i2/i.java i3/d.java i4/b.java i4/i.java i4/k.java i5/e.java i5/f.java i5/s.java ic/k.java ic/n.java j0/g.java j0/h.java j0/i.java j0/j.java j0/k.java j0/p.java j4/a.java j7/c.java jd/a.java jd/c.java jd/e.java je/o.java k/f.java k0/a.java k0/e.java k4/a0.java k4/j.java k4/k.java k4/m.java k7/o.java k8/b.java k9/a.java kc/f.java kc/g.java kc/h.java kc/j.java kd/b.java kd/c.java l4/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	l4/i.java l5/e.java l8/g.java l9/f.java ld/c.java lg/a.java lg/c.java lg/f.java m1/a.java m1/c.java m3/c.java m4/d.java m4/i.java m5/e.java m5/f.java m9/d0.java m9/q.java mc/g.java mc/i.java md/c.java mv/b.java n1/a.java n2/a0.java n2/c0.java n2/o.java n4/a.java nd/a0.java nd/c0.java nd/d0.java nd/f.java nd/f0.java nd/h0.java nd/j.java nd/k.java nd/l.java nd/l0.java nd/m.java nd/n.java nd/q.java nd/t.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				nd/x.java nd/y.java nd/z.java nf/a.java nf/b.java o0/k.java o1/a.java o1/c.java o1/g.java o1/i.java o1/j.java o1/k.java o1/l.java o1/n.java o1/o.java o4/c.java o4/e.java o4/s.java o5/c.java o7/c.java oa/i.java od/b.java od/e.java od/g.java of/d.java p/a.java p6/a.java p6/b.java p6/d.java p7/b.java p9/b.java pl/a.java q5/c.java q5/e.java q5/f.java q5/h.java q5/i.java q7/a.java q7/f.java q8/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				q8/b.java q8/d.java ql/j.java ql/l.java ql/q.java r0/c.java r1/a0.java r1/c0.java r1/d.java r1/e0.java r1/l.java r4/b.java r4/g.java r4/i.java r4/j.java r4/n.java r4/s.java r4/v.java r6/m.java r8/a.java r9/b.java r9/c.java r9/e.java r9/g.java r9/k.java r9/l.java r9/n.java r9/o.java r9/p.java rd/a.java s1/a.java s1/h.java s1/i.java s1/s.java s3/a.java s5/a.java s9/e.java s9/f.java s9/h.java s9/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				s9/p.java s9/t.java s9/y.java sa/a.java sb/a.java sc/e.java sd/a.java sd/b.java se/c.java t0/a.java t0/b.java t0/d0.java t0/f0.java t0/p.java t0/s0.java t5/a.java ta/d6.java ta/k6.java ta/r6.java ta/w2.java ta/x3.java td/b.java tr/r.java u1/b.java u1/c.java u4/a.java u4/e.java u7/b.java u7/o.java u8/a.java u8/c.java ua/a.java ub/e.java ud/c.java ud/d.java ue/b.java ur/a.java uv/h.java v/d.java v8/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				v9/b.java v9/c.java v9/d1.java v9/e.java v9/j0.java v9/q0.java v9/u0.java v9/v.java v9/y.java vb/b.java ve/c.java vv/d.java w/m.java w/p.java w2/f.java w2/l.java w2/n.java w4/d.java w4/i.java w4/j.java w4/m.java w5/u.java w5/w.java w6/a.java w8/c.java w8/d.java wa/a.java x0/b.java x1/h.java x1/i.java x1/k.java x1/n.java x1/o.java x8/a.java xa/a.java xd/e.java y6/f.java y7/a.java y8/e.java y8/f.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	y9/a.java y9/b.java z/b.java z/c.java z/d.java z4/h.java z7/d.java z8/a.java z8/c.java z9/a.java ze/c.java aa/a.java com/appsflyer/internal/AFb1tSDK.java com/bugsnag/android/DeliveryHeadersKt.java dl/n.java nd/f.java sc/b.java ue/b.java
4	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	bi/p.java c2/b.java i7/a.java j7/i.java je/l0.java je/s0.java je/v0.java je/x0.java k7/j.java k7/k.java k7/m.java k7/n.java k7/o.java k7/q.java lg/d.java p7/b.java ta/d6.java ta/k.java ta/l.java ta/q2.java ta/q6.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	com/canhub/cropper/CropImageActivity.java com/canhub/cropper/CropImageView.java com/theinnerhour/b2b/activity/WebviewActivity.java com/theinnerhour/b2b/components/chat/activity/CoachChatActivity.java com/theinnerhour/b2b/components/learningHub/experiment/activities/LearningHubArticleExperimentActivity.java com/theinnerhour/b2b/components/learningHub/experiment/activities/LearningHubExperimentVideoActivity.java com/theinnerhour/b2b/components/profile/experiment/activities/ExperimentEditProfileActivity.java com/theinnerhour/b2b/components/telecommunications/activity/TelecommunicationsPWAActivity.java ql/a0.java ue/c.java vm/b.java
6	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/canhub/cropper/d.java com/theinnerhour/b2b/activity/LearningHubArticleActivity.java com/theinnerhour/b2b/components/expertCare/activity/ExpertResourceActivity.java w5/e0.java
7	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	uv/c.java uv/d.java uv/g.java uv/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/theinnerhour/b2b/MyApplication.java g6/x.java h5/b.java h5/g0.java h5/i.java h5/y.java o5/g.java pn/a.java q3/b.java ql/e0.java s1/s.java u5/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/theinnerhour/b2b/fragment/coping/a.java com/theinnerhour/b2b/receiver/WorryTimeReceiver.java com/theinnerhour/b2b/service/MyFirebaseMessagingService.java cs/f.java cs/h.java fq/q0.java g6/b.java hd/g.java hr/p5.java hr/s7.java hr/v5.java j$/util/concurrent/ThreadLocalRandom.java ja/b.java jf/c.java nf/f.java o8/l.java p9/a.java ta/k6.java vc/a.java vr/h0.java vr/j0.java vr/v2.java vs/a.java vs/b.java wr/i.java ws/a.java yq/f.java
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/bugsnag/android/RootDetector.java hc/k.java kc/j.java nd/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	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	qk/c.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	com/appsflyer/internal/AFb1tSDK.java di/b.java i5/d.java q5/i.java ta/k6.java
13	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/theinnerhour/b2b/activity/BotPwaActivity.java com/theinnerhour/b2b/activity/WebviewActivity.java com/theinnerhour/b2b/components/community/activity/CommunitiesPwaActivity.java com/theinnerhour/b2b/components/login/activity/SSOLoginPWA.java com/theinnerhour/b2b/components/telecommunications/activity/TelecommunicationsPWAActivity.java ni/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
14	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/theinnerhour/b2b/activity/BotPwaActivity.java com/theinnerhour/b2b/activity/WebviewActivity.java com/theinnerhour/b2b/components/community/activity/CommunitiesPwaActivity.java com/theinnerhour/b2b/components/telecommunications/activity/TelecommunicationsPWAActivity.java di/b.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/x86/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strncat_chk', '__memcpy_chk']	True info Symbols are stripped.
2	lib/x86/libbugsnag-root-detection.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/x86/libbugsnag-ndk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
4	lib/x86/libbugsnag-plugin-android-anr.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/x86_64/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strncat_chk', '__memcpy_chk']	True info Symbols are stripped.
6	lib/x86_64/libbugsnag-root-detection.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	lib/x86_64/libbugsnag-ndk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsprintf_chk', '__read_chk', '__strcpy_chk', '__strlen_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.
8	lib/x86_64/libbugsnag-plugin-android-anr.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	lib/armeabi-v7a/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strncat_chk', '__memcpy_chk']	True info Symbols are stripped.
10	lib/armeabi-v7a/libbugsnag-root-detection.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	lib/armeabi-v7a/libbugsnag-ndk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
12	lib/armeabi-v7a/libbugsnag-plugin-android-anr.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	lib/arm64-v8a/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strncat_chk']	True info Symbols are stripped.
14	lib/arm64-v8a/libbugsnag-root-detection.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	lib/arm64-v8a/libbugsnag-ndk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsprintf_chk', '__read_chk', '__strcpy_chk', '__strlen_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.
16	lib/arm64-v8a/libbugsnag-plugin-android-anr.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	lib/x86/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strncat_chk', '__memcpy_chk']	True info Symbols are stripped.
18	lib/x86/libbugsnag-root-detection.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	lib/x86/libbugsnag-ndk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
20	lib/x86/libbugsnag-plugin-android-anr.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	lib/x86_64/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strncat_chk', '__memcpy_chk']	True info Symbols are stripped.
22	lib/x86_64/libbugsnag-root-detection.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	lib/x86_64/libbugsnag-ndk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsprintf_chk', '__read_chk', '__strcpy_chk', '__strlen_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.
24	lib/x86_64/libbugsnag-plugin-android-anr.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
25	lib/armeabi-v7a/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strncat_chk', '__memcpy_chk']	True info Symbols are stripped.
26	lib/armeabi-v7a/libbugsnag-root-detection.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
27	lib/armeabi-v7a/libbugsnag-ndk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
28	lib/armeabi-v7a/libbugsnag-plugin-android-anr.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	lib/arm64-v8a/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strncat_chk']	True info Symbols are stripped.
30	lib/arm64-v8a/libbugsnag-root-detection.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	lib/arm64-v8a/libbugsnag-ndk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsprintf_chk', '__read_chk', '__strcpy_chk', '__strlen_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.
32	lib/arm64-v8a/libbugsnag-plugin-android-anr.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
sonelink.s	ok	No Geolocation information available.
sinapps.s	ok	No Geolocation information available.
developer.apple.com	ok	**IP:** 17.253.97.205 **Country:** United States of America **Region:** New Jersey **City:** Newark **Latitude:** 40.735661 **Longitude:** -74.172371 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.oxfordsparks.ox.ac.uk	ok	**IP:** 77.68.29.153 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Gloucester **Latitude:** 51.865681 **Longitude:** -2.243100 **View:** Google Map
sstats.s	ok	No Geolocation information available.
app-measurement.com	ok	No Geolocation information available.
sars.s	ok	No Geolocation information available.
www.amahahealth.com	ok	**IP:** 34.93.132.182 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.014410 **Longitude:** 72.847939 **View:** Google Map
plus.google.com	ok	**IP:** 142.250.81.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
.facebook.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
bot.theinnerhour.com	ok	**IP:** 35.200.142.92 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.014410 **Longitude:** 72.847939 **View:** Google Map
cdn-settings.s	ok	No Geolocation information available.
assets.theinnerhour.com	ok	**IP:** 13.225.214.120 **Country:** United States of America **Region:** New Jersey **City:** Newark **Latitude:** 40.735661 **Longitude:** -74.172371 **View:** Google Map
api.theinnerhour.com	ok	**IP:** 34.93.132.182 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.014410 **Longitude:** 72.847939 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebase.google.com	ok	**IP:** 142.251.40.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.googleadservices.com	ok	No Geolocation information available.
sattr.s	ok	No Geolocation information available.
google.com	ok	**IP:** 142.250.65.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
slaunches.s	ok	No Geolocation information available.
ipinfo.io	ok	No Geolocation information available.
www.facebook.com	ok	**IP:** 157.240.241.35 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ssdk-services.s	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.
developers.facebook.com	ok	**IP:** 157.240.241.17 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
accounts.google.com	ok	**IP:** 142.251.40.141 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
play.google.com	ok	**IP:** 142.250.65.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
facebook.com	ok	**IP:** 157.240.241.35 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
us-central1-gcpinnerhour.cloudfunctions.net	ok	**IP:** 216.239.36.54 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
svalidate.s	ok	No Geolocation information available.
api2.amplitude.com	ok	No Geolocation information available.
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	**IP:** 142.250.81.228 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gl	ok	**IP:** 142.251.40.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
graph-video.s	ok	No Geolocation information available.
maps.google.com	ok	**IP:** 142.250.64.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sregister.s	ok	No Geolocation information available.
api.mixpanel.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
docs.bugsnag.com	ok	**IP:** 13.33.82.5 **Country:** United States of America **Region:** New Jersey **City:** Newark **Latitude:** 40.735661 **Longitude:** -74.172371 **View:** Google Map
creativecommons.org	ok	**IP:** 172.67.34.140 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
aomedia.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
graph.s	ok	No Geolocation information available.
bit.ly	ok	**IP:** 67.199.248.11 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sviap.s	ok	No Geolocation information available.
gcpinnerhour.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
api.eu.amplitude.com	ok	**IP:** 52.58.122.110 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
prodicus.netlify.app	ok	**IP:** 54.84.236.175 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
smonitorsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
notify.theinnerhour.com	ok	**IP:** 104.199.253.255 **Country:** Taiwan (Province of China) **Region:** Taipei **City:** Taipei **Latitude:** 25.047760 **Longitude:** 121.531853 **View:** Google Map
sapp.s	ok	No Geolocation information available.
cdn-testsettings.s	ok	No Geolocation information available.
firebaseappcheck.googleapis.com	ok	**IP:** 142.250.65.170 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
nitro.theinnerhour.com	ok	**IP:** 35.196.223.198 **Country:** United States of America **Region:** South Carolina **City:** North Charleston **Latitude:** 32.888561 **Longitude:** -80.007507 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
notify.bugsnag.com	ok	**IP:** 35.186.205.6 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.
console.firebase.google.com	ok	**IP:** 142.251.40.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sessions.bugsnag.com	ok	**IP:** 35.190.88.7 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
sadrevenue.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.theinnerhour.com	ok	**IP:** 34.93.157.126 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.014410 **Longitude:** 72.847939 **View:** Google Map
bugsnag.com	ok	No Geolocation information available.
community.amahahealth.com	ok	**IP:** 34.93.132.182 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.014410 **Longitude:** 72.847939 **View:** Google Map
firebase-settings.crashlytics.com	ok	No Geolocation information available.
innerhour.page.link	ok	**IP:** 142.250.80.65 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sconversions.s	ok	No Geolocation information available.
pagead2.googlesyndication.com	ok	No Geolocation information available.

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://gcpinnerhour.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	s9/r.java
this@v3goalsactivity.displaydat	am/c0.java
this@v3goalsactivity.displaydat	am/d0.java
support@amahahealth.com	ho/z.java
this@splashscreenactivity.window	com/theinnerhour/b2b/components/splash/activity/SplashScreenActivity.java
this@notv4activity.applicatio	com/theinnerhour/b2b/components/dashboard/experiment/activity/NotV4Activity.java
support@amahahealth.com	com/theinnerhour/b2b/activity/FAQActivity.java
support@amahahealth.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Bugsnag	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/207
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
MixPanel	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/118
MoEngage	Analytics	https://reports.exodus-privacy.eu.org/trackers/268

HARDCODED SECRETS

POSSIBLE SECRETS
"com_facebook_device_auth_instructions" : "□□facebook.com/device□□□□□□□□□□□□□□"
"facebook_client_token" : "f7bfe92c82485f7c21250ab1130be4a2"
"google_api_key" : "AIzaSyCxHzUlmB4Lt_sK710XZDh9lIgmvxFh3QU"

POSSIBLE SECRETS
"MIXPANEL_TOKEN" : "2c3f665efcaf962a258c3da5c8bafa22"
"google_crash_reporting_api_key" : "AIzaSyCxHzUlmB4Lt_sK710XZDh9lIgmvxFh3QU"
"firebase_database_url" : "https://gcpinnerhour.firebaseio.com"
"com_facebook_device_auth_instructions" : "facebook.com/device□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"com.google.firebase.crashlytics.mapping_file_id" : "91eed46f4d594043bab2819a11565c26"
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
99577353-fd79-4470-943d-1bd65e2a1a2f
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
782730c9-04c0-4fb5-81e8-6f2739e1d8d9
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
84982153-2f9c-4982-9bd1-f5a614d96456
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
113aaa66-887f-11ea-bc55-0242ac130003
28caa46a6e9c77fbe291287e4fec061f
470fa2b4ae81cd56ecbcda9735803434cec591fa
Xa20frT4BnvlDzUFMmorgwJFMcI
07cd8acb-c988-49fe-9bad-9b3683ff26f0
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
9b8f518b086098de3d77736f9458a3d2f6f95a37
115792089210356248762697446949407573529996955224135760342422259061068512044369
85053bf24bba75239b16a601d9387e17
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
db992ff7-a994-499c-a05b-3c3cb44fdfb5
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F

POSSIBLE SECRETS
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
cc2751449a350f668590264ed76692694a80308a
ae2044fb577e65ee8bb576ca48a2f06e
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
5181942b9ebc31ce68dacb56c16fd79f
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
25a56fe2-6361-4ab5-a04a-dd00a9e50766
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
c56fb7d591ba6704df047fd98f535372fea00211
33b80e0a-267a-49b4-9a80-2d87dce7f99a

POSSIBLE SECRETS
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
16112da6-637b-48a1-915f-0112aca125ed

Report Generated by - MobSF v3.7.9 Beta

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.