

ANDROID STATIC ANALYSIS REPORT



Anime Witcher (1.2.2)

File Name:	Anime Witcher_1.2.2.apk
Package Name:	com.anime.witcher
Scan Date:	Sept. 27, 2024, 1:40 a.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	7/432

FINDINGS SEVERITY

≟ HIGH	▲ MEDIUM	i INFO	✓ SECURE	® HOTSPOT
7	57	2	2	1

FILE INFORMATION

File Name: Anime Witcher_1.2.2.apk

Size: 18.86MB

MD5: bed939ba3cb40df4e267164d7f4f303c

SHA1: c3d401442d12e7c2b8dcf58e9aa22f9b9f916f55

SHA256: 7ba8039404de76bde730ebc6e6344ee6d5060d39f0126a9d74cd6ce1cd32de76

i APP INFORMATION

App Name: Anime Witcher

Package Name: com.anime.witcher

Main Activity: com.example.animewitcher.HomeActivity

Target SDK: 34 Min SDK: 21 Max SDK:

Android Version Name: 1.2.2

EE APP COMPONENTS

Activities: 82 Services: 19 Receivers: 17 Providers: 5

Exported Activities: 31
Exported Services: 2
Exported Receivers: 8
Exported Providers: 0



Binary is signed v1 signature: True v2 signature: True v3 signature: False v4 signature: False

X.509 Subject: CN=Android Debug, O=Android, C=US

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2021-08-11 11:37:02+00:00 Valid To: 2051-08-04 11:37:02+00:00

Issuer: CN=Android Debug, O=Android, C=US

Serial Number: 0x1 Hash Algorithm: sha1

md5: d920b6b92cdd171613b77e281c410539

sha1: 6e67d0fede39b63279703d45b626e9f1feccc521

sha256: 2da9f933f18714cad0758766d970afd67385cb8964cdb717a75a3b10af2d09b8

sha512: aec52586056f949fd43921d1fe10ab6436d46f3d3e03b3e2097e5d99c99fe4838924f8792e094616a34464166c559db90f54dcdf19cbc53e8b7a0f363574eee8

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 6374ca2d8f7e07c5acd801d299c1b55722e6b200a54c02c2bd5c57ed041a0ac0

Found 1 unique certificates

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.Ad_ID	unknown	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
com.anime.witcher.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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
com.applovin.array.apphub.permission.BIND_APPHUB_SERVICE	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.

PERMISSION	STATUS	INFO	DESCRIPTION
com.anime.witcher.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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.

M APKID ANALYSIS

FILE	DETAILS	
classes13.dex	FINDINGS	DETAILS
Classes IS. dex	Compiler	r8 without marker (suspicious)
classes4.dex	FINDINGS	DETAILS
Compiler	Compiler	r8 without marker (suspicious)
classes11.dex	FINDINGS	DETAILS
Classes I I.acx	Compiler	r8 without marker (suspicious)

FILE	DETAILS			
	FINDINGS	DETAILS		
classes15.dex	Compiler	r8 without marker (susp	picious)	
classes12.dex	FINDINGS	DETAILS		
Classes (2. acx	Compiler	r8 without marker (susp	picious)	
classes14.dex	FINDINGS DETAILS		DETAILS	
Classes Findex	Compiler	r8 without marker (suspicious)		
classes2.dex	FINDINGS		DETAILS	
	Compiler		dx	
classes16.dex	FINDINGS DETAILS			
	Compiler r8 without marker (su		picious)	

FILE	DETAILS		
classes3.dex	FINDINGS	DETAILS	
Classess.ucx	Compiler	r8 without marker (suspicious)	
	FINDINGS	DETAILS	
classes7.dex	Compiler	r8 without marker (suspicious)	
classes5.dex	FINDINGS	DETAILS	
	Compiler	r8 without marker (suspicious)	
classes10.dex	FINDINGS	DETAILS	
Classes To. dex	Compiler	r8 without marker (suspicious)	

FILE	DETAILS		
	FINDINGS	DETAILS	
classes17.dex	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.TAGS check SIM operator check	
	Compiler	r8 without marker (suspicious)	
	FINDINGS	DETAILS	
classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check network operator name check possible VM check	
	Compiler	r8 without marker (suspicious)	
classes8.dex	FINDINGS	DETAILS	
	Compiler	r8 without marker (suspicious)	

FILE	DETAILS	
classes6.dex	FINDINGS	DETAILS
ciasseso.uex	Compiler	r8 without marker (suspicious)
classes9.dex	FINDINGS	DETAILS
classess.aex	Compiler	r8 without marker (suspicious)
	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check ro.hardware check ro.product.device check possible ro.secure check emulator file check possible VM check
classes18.dex	Anti Debug Code	Debug.isDebuggerConnected() check

FILE	D ETIMIDUS IGS	DETAILS		
	Compiler	r8 without marker (suspicious)		
	FINDINGS	DETAILS		
classes19.dex				
	Compiler	r8 without marker (suspicious)		

■ BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,

ACTIVITY	INTENT
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

△ NETWORK SECURITY

NO S	SCOPE	SEVERITY	DESCRIPTION
------	-------	----------	-------------

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 2 | 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.
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

Q MANIFEST ANALYSIS

HIGH: 3 | WARNING: 43 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	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	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.
4	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
5	Activity (com.example.animewitcher.activites.SeasonsActivity) 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
6	Activity (com.example.animewitcher.activites.UserCommentsActivity) 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.
7	Activity (com.example.animewitcher.activites.SearchCharactersActivity) 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	Activity (com.example.animewitcher.activites.CharactersByldsActivity) 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.
9	Activity (com.example.animewitcher.characters.ViewCharacterActivity) 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.
10	Activity (com.example.animewitcher.activites.LastWatchedActivity) 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.
11	Activity (com.example.animewitcher.activites.AddCommentActivity) 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.
12	Activity (com.example.animewitcher.activites.ViewImageActivity) 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	Activity (com.example.animewitcher.activites.CommentsActivity) 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
14	Activity (com.example.animewitcher.animelist.ranking.AnimeRankingActivity) 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.
15	Activity (com.example.animewitcher.reviews.AnimeReviewsActivity) 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.
16	Activity (com.example.animewitcher.activites.ServersActivity) 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.
17	Activity (com.example.animewitcher.activites.RepliesActivity) 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.
18	Activity (com.example.animewitcher.user.EditUserInfoActivity) 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.
19	Activity (com.example.animewitcher.user.notifications.NotificationsActivity) 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.
20	Activity (com.example.animewitcher.tags_search.TagSearchActivity) 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.
21	Activity (com.example.animewitcher.reviews.UserReviewsActivity) 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
22	Activity (com.example.animewitcher.activites.AddReviewActivity) 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.
23	Activity (com.example.animewitcher.user.user_animes.UserAnimeActivity) 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.
24	Activity (com.example.animewitcher.wallpapers.WallpapersActivity) 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.
25	Activity (com.example.animewitcher.activites.FavAnimeActivity) 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.
26	Activity (com.example.animewitcher.activites.UserProfileActivity) 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.
27	Activity (com.example.animewitcher.FreeResActivity) 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.
28	Activity (com.example.animewitcher.CallUsActivity) 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.
29	Activity (com.example.animewitcher.activites.SettingsActivity) 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
30	Activity (com.example.animewitcher.SplashActivity) 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.
31	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.
32	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.
33	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.
34	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.
35	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.

NO	ISSUE	SEVERITY	DESCRIPTION
36	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.
37	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.
38	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.
39	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.
40	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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
41	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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.
42	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.
43	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.
44	Broadcast Receiver (com.startapp.sdk.adsbase.remoteconfig.BootCompleteListener) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
45	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.
46	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: 2 | WARNING: 11 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/airbnb/lottie/LottieCompositionFactory.java com/algolia/search/saas/android/BuildConfig.java com/applovin/impl/ig.java com/applovin/impl/sdk/AppLovinSdkInitialization ConfigurationImpl.java com/applovin/impl/sdk/k.java com/applovin/mediation/ads/MaxAdView.java com/applovin/mediation/ads/MaxAppOpenAd.jav a com/applovin/mediation/ads/MaxInterstitialAd.ja va com/applovin/mediation/ads/MaxRewardedAd.ja

NO	ISSUE	SEVERITY	STANDARDS	FOM/applovin/mediation/ads/MaxRewardedInters titialAd.java
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	com/applovin/mediation/nativeAds/MaxNativeAd Loader.java com/applovin/sdk/AppLovinSdk.java com/applovin/sdk/AppLovinSdkSettings.java com/applovin/sdk/AppLovinSdkSettings.java com/applovin/sdk/AppLovinWebViewActivity.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCache Key.java com/bumptech/glide/manager/RequestManagerRetriever.java com/chivorn/smartmaterialspinner/SearchableSpinnerDialog.java com/example/animewitcher/utils/SharedPrefHelper.java com/onesignal/FCMBroadcastReceiver.java com/onesignal/NotificationBundleProcessor.java com/onesignal/OSInAppMessageController.java com/onesignal/OSInAppMessageController.java com/onesignal/OSInAppMessagePrompt.java com/onesignal/OSInAppMessagePrompt.java com/onesignal/OSInAppMessagePrompt.java com/onesignal/OSNotification.java com/onesignal/OSNotificationController.java com/onesignal/OSSMSSubscriptionState.java com/onesignal/OSSMSSubscriptionState.java com/onesignal/OSSWSSubscriptionState.java com/onesignal/OSSWSSubscriptionState.java com/onesignal/OSSWSSubscriptionState.java com/onesignal/OSSignalHmsEventBridge.java com/onesignal/OneSignalHmsEventBridge.java com/onesignal/OneSignalRemoteParams.java com/onesignal/UserState.java

NO	ISSUE	SEVERITY	STANDARDS	com/onesignal/OserStatesynchronizer.java မှာကု£ဇွာesignal/WebViewManager.java com/unity3d/ads/metadata/InAppPurchaseMetaD
				ata.java com/unity3d/services/ads/gmascar/utils/ScarCons tants.java com/unity3d/services/core/configuration/Experim entObject.java com/unity3d/services/core/device/reader/Devicel nfoReaderFilterProvider.java com/unity3d/services/core/device/reader/JsonSto rageKeyNames.java com/unity3d/services/core/properties/SdkPropert ies.java io/grpc/PersistentHashArrayMappedTrie.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/TransportFrameUtil.java org/litepal/util/cipher/CipherUtil.java
				com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/algolia/search/saas/FutureRequest.java com/applovin/impl/rc.java com/applovin/impl/sdk/t.java com/applovin/impl/tg.java com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.j ava com/bumptech/glide/gifdecoder/GifHeaderParser. java com/bumptech/glide/gifdecoder/StandardGifDeco der.java com/bumptech/glide/load/data/AssetPathFetcher. java com/bumptech/glide/load/data/HttpUrlFetcher.ja va com/bumptech/glide/load/data/LocalUriFetcher.ja va com/bumptech/glide/load/data/LocalUriFetcher.ja va com/bumptech/glide/load/data/mediastore/Thum

NO	ISSUE	SEVERITY	STANDARDS	bFetcher.java File 5 umptech/glide/load/data/mediastore/Thum bnailStreamOpener.java
				com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.jav

NO	ISSUE	SEVERITY	STANDARDS	com/bumptech/glide/load/resource/bitmap/Hard
				com/bumptech/glide/load/resource/bitmap/Trans
				formationUtils.java
				com/bumptech/glide/load/resource/bitmap/Video
				Decoder.java
				com/bumptech/glide/load/resource/gif/ByteBuffe
				rGifDecoder.java
				com/bumptech/glide/load/resource/gif/GifDrawa
				bleEncoder.java
				com/bumptech/glide/load/resource/gif/StreamGif
				Decoder.java
				com/bumptech/glide/manager/DefaultConnectivit
				yMonitor.java
				com/bumptech/glide/manager/DefaultConnectivit
				yMonitorFactory.java
				com/bumptech/glide/manager/RequestManagerFr
				agment.java
				com/bumptech/glide/manager/RequestManagerR
				etriever.java
				com/bumptech/glide/manager/RequestTracker.jav
				a
				com/bumptech/glide/manager/SupportRequestM
				anagerFragment.java
				com/bumptech/glide/module/ManifestParser.java
				com/bumptech/glide/request/SingleRequest.java
				com/bumptech/glide/request/target/CustomView
				Target.java
				com/bumptech/glide/request/target/ViewTarget.ja
				va
				com/bumptech/glide/signature/ApplicationVersio
				nSignature.java
				com/bumptech/glide/util/ContentLengthInputStre
				am.java
				com/bumptech/glide/util/pool/FactoryPools.java
				com/example/animewitcher/HomeActivity.java
				com/example/animewitcher/SaveImage.java
				com/example/animewitcher/activites/AnimeDetail
				sActivity.java
				com/example/animewitcher/activites/RepliesActiv

NO	ISSUE	SEVERITY	STANDARDS	ity.java Fd h
				com/example/animewitcher/activites/StreamActiv
				ity.java
				com/example/animewitcher/activites/news/Showl
				nterstitialAd.java
				com/example/animewitcher/activites/sign_user/S
				ocialSignInActivity.java
				com/example/animewitcher/characters/Character
				sFragment.java
				com/example/animewitcher/reviews/ReviewsAda
				pter.java
				com/example/animewitcher/reviews/WrapConten
				tLinearLayoutManager.java
				com/example/animewitcher/user/EditUserInfoActi
				vity.java
				com/example/animewitcher/utils/StaticMethods.j
				ava
				com/iab/omid/library/applovin/publisher/b.java
				com/iab/omid/library/applovin/utils/d.java
				com/iab/omid/library/startio/publisher/b.java
				com/iab/omid/library/startio/utils/d.java
				com/koushikdutta/async/AsyncNetworkSocket.jav a
				com/koushikdutta/async/AsyncServer.java
				com/koushikdutta/async/ByteBufferList.java
				com/koushikdutta/async/PushParser.java
				com/koushikdutta/async/Util.java
				com/koushikdutta/async/http/AsyncHttpRequest.j
				ava
				com/koushikdutta/async/http/HybiParser.java
				com/koushikdutta/async/http/cache/RawHeaders.
				java
				com/koushikdutta/async/http/server/AsyncHttpSe
				rver.java
				com/koushikdutta/async/http/server/AsyncHttpSe
				rverRequestImpl.java
				com/koushikdutta/async/http/server/AsyncHttpSe
				rverRouter.java

NO	ISSUE	SEVERITY	STANDARDS	com/koushikdutta/ion/lon.java Ght Soushikdutta/ion/lonLog.java com/koushikdutta/ion/lonReguestBuilder.java
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	com/koushikdutta/ion/bitmap/Exif.java com/koushikdutta/ion/bitmap/IonBitmapCache.ja va com/koushikdutta/ion/conscrypt/ConscryptMiddl eware.java com/koushikdutta/ion/cookie/CookieMiddleware.j ava com/koushikdutta/ion/gif/GifDecoder.java com/onesignal/AndroidSupportV4Compat.java com/onesignal/JobIntentService.java com/onesignal/JobIntentService.java com/onesignal/JobIntentService.java com/onesignal/JobIntentService.java com/onesignal/JobIntentService.java com/onesignal/JobIntentService.java com/onesignal/JobIntentService.java com/onesignal/JobIntentService.java com/onesignal/JobIntentService.java com/onesignal/Shortcutbadger/ShortcutBadger.ja va com/startapp/d1.java com/startapp/d1.java com/startapp/sdk/ads/splash/SplashConfig.java com/startapp/sdk/ads/splash/SplashConfig.java com/startapp/sdk/ads/splash/SplashConfig.java com/startapp/sdk/ads/splash/SplashConfig.java com/theartofdev/edmodo/cropper/BitmapUtils.ja va com/theartofdev/edmodo/cropper/CropImageActi vity.java com/unity3d/ads/UnityAdsBaseOptions.java com/unity3d/ads/metadata/InAppPurchaseMetaD ata.java com/unity3d/ads/metadata/MetaData.java com/unity3d/ads/metadata/MetaData.java com/unity3d/services/ads/UnityAdsImplementati on.java com/unity3d/services/ads/JunityAdsImplementati on.java com/unity3d/services/ads/adunit/AdUnitActivityC ontroller.java com/unity3d/services/ads/adunit/AdUnitViewHan dlerFactory.java com/unity3d/services/ads/adunit/VideoPlayerHan

NO	ISSUE	SEVERITY	STANDARDS	dler.java Fdht Snity3d/services/ads/api/AdUnit.java com/unity3d/services/ads/api/VideoPlayer.java
				com/unity3d/services/ads/api/WebPlayer.java com/unity3d/services/ads/gmascar/adapters/Scar AdapterFactory.java com/unity3d/services/ads/gmascar/bridges/Adapt erStatusBridge.java com/unity3d/services/ads/gmascar/bridges/Initial izeListenerBridge.java com/unity3d/services/ads/gmascar/bridges/mobil eads/MobileAdsBridge.java com/unity3d/services/ads/gmascar/bridges/mobil eads/MobileAdsBridgeLegacy.java com/unity3d/services/ads/gmascar/finder/GMAIni tializer.java com/unity3d/services/ads/gmascar/finder/ScarVe rsionFinder.java com/unity3d/services/ads/token/InMemoryAsync TokenStorage.java
				com/unity3d/services/ads/token/NativeTokenGen erator.java com/unity3d/services/ads/topics/TopicsReceiver.j ava com/unity3d/services/ads/topics/TopicsService.ja va com/unity3d/services/ads/video/VideoPlayerView. java com/unity3d/services/ads/webplayer/WebPlayerV iew.java com/unity3d/services/banners/BannerView.java com/unity3d/services/banners/UnityBanners.java com/unity3d/services/core/api/Cache.java com/unity3d/services/core/api/DeviceInfo.java com/unity3d/services/core/api/Intent.java com/unity3d/services/core/api/Request.java com/unity3d/services/core/api/Sdk.java com/unity3d/services/core/broadcast/BroadcastE ventReceiver.java com/unity3d/services/core/cache/CacheDirectory.

OV	ISSUE	SEVERITY	STANDARDS	java Edu ZS nity3d/services/core/cache/CacheThread.ja
				com/unity3d/services/core/cache/CacheThreadHa
				ndler.java
				com/unity3d/services/core/configuration/Configu
				rationReader.java
				com/unity3d/services/core/configuration/Configu
				rationRequestFactory.java
				com/unity3d/services/core/configuration/Environ
				mentCheck.java
				com/unity3d/services/core/configuration/Experim
				entObject.java
				com/unity3d/services/core/configuration/Experim
				entsReader.java
				com/unity3d/services/core/configuration/Initializa
				tionNotificationCenter.java
				com/unity3d/services/core/configuration/Initialize
				EventsMetricSender.java
				com/unity3d/services/core/configuration/Initialize
				Thread.java
				com/unity3d/services/core/configuration/Privacy ConfigurationLoader.java
				com/unity3d/services/cornectivity/Connecti
				vityMonitor.java
				com/unity3d/services/core/device/AdvertisingId.ja
				va
				com/unity3d/services/core/device/Device.java
				com/unity3d/services/core/device/OpenAdvertisi
				ngld.java
				com/unity3d/services/core/device/Storage.java
				com/unity3d/services/core/device/reader/Devicel
				nfoReaderCompressor.java
				com/unity3d/services/core/device/reader/Devicel
				nfoReaderExtended.java
				com/unity3d/services/core/domain/task/Initialize
				SDK\$doWork\$2.java
				com/unity3d/services/core/domain/task/Initialize
				StateConfig\$doWork\$2.java
				com/unity3d/services/core/domain/task/Initialize

NO	ISSUE	SEVERITY	STANDARDS	StateCreate\$doWork\$2.java Fdbf5nity3d/services/core/domain/task/Initialize StateCreateWithRemote\$doWork\$2.java
				com/unity3d/services/core/domain/task/Initialize
				StateError\$doWork\$2.java
				com/unity3d/services/core/domain/task/Initialize
				StateLoadCache\$doWork\$2.java
				com/unity3d/services/core/domain/task/Initialize
				StateLoadCache.java
				com/unity3d/services/core/domain/task/Initialize
				StateLoadWeb\$doWork\$2.java
				com/unity3d/services/core/domain/task/Initialize
				StateNetworkError\$doWork\$2.java
				com/unity3d/services/core/domain/task/Initialize
				StateNetworkError.java
				com/unity3d/services/core/domain/task/Initialize
				StateReset\$doWork\$2.java
				com/unity3d/services/core/extensions/TaskExtens
				ionsKt.java
				com/unity3d/services/core/log/DeviceLog.java
				com/unity3d/services/core/misc/JsonFlattener.jav
				a
				com/unity3d/services/core/misc/JsonStorage.java
				com/unity3d/services/core/misc/JsonStorageAggr
				egator.java
				com/unity3d/services/core/misc/Utilities.java
				com/unity3d/services/core/misc/ViewUtilities.java
				com/unity3d/services/core/preferences/AndroidP
				references.java
				com/unity3d/services/core/properties/ClientProp
				erties.java
				com/unity3d/services/core/properties/SdkPropert
				ies.java
				com/unity3d/services/core/reflection/GenericBrid
				ge.java
				com/unity3d/services/core/request/WebRequest.j
				ava
				com/unity3d/services/core/request/WebRequestR
				unnable.java com/unity3d/services/core/request/WebRequestT
				com/unity5u/services/core/request/webkequest1

NO	ISSUE	SEVERITY	STANDARDS	hread.java
				com/unity3d/services/core/request/metrics/Metricsender\$sendMetrics\$\$inlined\$CoroutineExceptio
				nHandler\$1.java
				com/unity3d/services/core/request/metrics/Metri
				cSender\$sendMetrics\$1.java
				com/unity3d/services/core/request/metrics/Metri cSender.java
				com/unity3d/services/core/request/metrics/Metr
				com/unity3d/services/core/request/metrics/SDK
				Metrics.java
				com/unity3d/services/core/sensorinfo/SensorInfo
				Listener.java
				com/unity3d/services/core/timer/BaseTimer.java
				com/unity3d/services/core/webview/WebView.jav
				a
				com/unity3d/services/core/webview/WebViewAp
				p.java
				com/unity3d/services/core/webview/WebViewUrl
				Builder.java
				com/unity3d/services/core/webview/bridge/Invocation.java
				com/unity3d/services/core/webview/bridge/NativeCallback.java
				com/unity3d/services/core/webview/bridge/WebV
				iewBridge.java
				com/unity3d/services/core/webview/bridge/WebV
				iewBridgeInterface.java
				com/unity3d/services/core/webview/bridge/WebV
				iewCallback.java
				com/unity3d/services/store/core/StoreLifecycleLis tener.java
				com/unity3d/services/store/gpbl/bridges/Commo
				nJsonResponseBridge.java
				com/unity3d/services/store/gpbl/bridges/Purchas
				eBridge.java
				io/grpc/android/AndroidChannelBuilder.java

NO-	ISSUE	SEVERITY	STANDARDS	io/grpc/okhttp/internal/Platform.java File/IiSpal/crud/DataHandler.java ess/literal/grud/Wayerlawdlar.java
3	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	ess/liferal/antessenter(//saneriation/religion/antessenter) ess/liferal/antessenter(//saneriation/astessenter) ess/liferal/antessenter(//saneriation/astessenter) ess/liferal/antesses/liferal/an
4	Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system.	warning	CWE: CWE-200: Information Exposure OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/unity3d/services/core/webview/WebView.jav a

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/applovin/impl/wq.java com/applovin/impl/zj.java com/example/animewitcher/HomeActivity.java com/example/animewitcher/activites/AnimeDetail sActivity.java com/example/animewitcher/activites/ServersActiv ity.java com/example/animewitcher/wallpapers/Wallpape rsActivity.java com/example/animewitcher/wallpapers/Wallpape rsActivity.java com/koushikdutta/async/dns/Dns.java com/koushikdutta/async/dns/Dns.java com/onesignal/GenerateNotification.java com/onesignal/OSUtils.java com/onesignal/OSUtils.java com/startapp/sdk/ads/banner/BannerBase.java com/startapp/sdk/ads/base/cache/d.java com/startapp/sdk/adsbase/cache/d.java com/startapp/sdk/adsbase/cache/g.java com/startapp/sdk/adsbase/cache/g.java com/unity3d/services/core/request/metrics/SDK Metrics.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/RetriableStream.java io/grpc/okhttp/OkHttpClientTransport.java io/grpc/okhttp/OkHttpClientTransport.java io/grpc/util/OutlierDetectionLoadBalancer.java io/grpc/util/RoundRobinLoadBalancer.java
6	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/example/animewitcher/Savelmage.java com/startapp/u5.java com/theartofdev/edmodo/cropper/BitmapUtils.ja va com/theartofdev/edmodo/cropper/CropImageActi vity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/example/animewitcher/Savelmage.java com/example/animewitcher/wallpapers/SaveAnd Share2.java com/startapp/c2.java com/unity3d/services/core/cache/CacheDirectory. java in/myinnos/savebitmapandsharelib/SaveAndShar e.java org/litepal/Operator.java org/litepal/tablemanager/Connector.java
8	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/example/animewitcher/activites/AnimeDetail sActivity.java com/startapp/d.java
9	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/applovin/impl/sdk/utils/StringUtils.java com/applovin/impl/wi.java com/koushikdutta/async/http/WebSocketImpl.jav a com/unity3d/services/core/device/Device.java
10	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/onesignal/OneSignalDbHelper.java com/onesignal/outcomes/data/OSOutcomeTableP rovider.java com/startapp/f6.java com/startapp/o3.java org/litepal/Operator.java org/litepal/tablemanager/AssociationCreator.java org/litepal/tablemanager/Generator.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/applovin/mediation/adapters/NimbusMediat ionAdapter.java com/koushikdutta/async/AsyncSSLSocketWrapper .java com/koushikdutta/async/dns/Dns.java com/startapp/c2.java com/startapp/kb.java io/grpc/okhttp/OkHttpClientTransport.java io/grpc/okhttp/OkHttpServerTransport.java
12	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/koushikdutta/async/AsyncSSLSocketWrapper .java com/koushikdutta/ion/lon.java io/grpc/okhttp/OkHttpChannelBuilder.java io/grpc/okhttp/OkHttpServerBuilder.java io/grpc/util/AdvancedTlsX509TrustManager.java
13	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/applovin/impl/cs.java com/applovin/impl/i0.java com/onesignal/WebViewManager.java
14	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/startapp/a7.java com/startapp/z6.java
15	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/startapp/a7.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
16	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/bumptech/glide/BuildConfig.java com/bumptech/glide/gifdecoder/BuildConfig.java com/example/animewitcher/BuildConfig.java
17	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/koushikdutta/async/util/FileCache.java com/startapp/sdk/ads/video/f.java org/litepal/util/cipher/CipherUtil.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
----	---------------	----	-----------------	-------	-------	---------	---------	---------------------

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	x86_64/libapplovin-native- crash-reporter.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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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: ['vsnprintf_chk', 'strlen_chk', 'memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	armeabi-v7a/libapplovin- native-crash-reporter.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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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: ['vsnprintf_chk', 'strlen_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	arm64-v8a/libapplovin- native-crash-reporter.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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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: ['vsnprintf_chk', 'strlen_chk', 'memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86/libapplovin-native-crash- reporter.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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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: ['vsnprintf_chk', 'strlen_chk', 'memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	x86_64/libapplovin-native- crash-reporter.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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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: ['vsnprintf_chk', 'strlen_chk', 'memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	armeabi-v7a/libapplovin- native-crash-reporter.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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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: ['vsnprintf_chk', 'strlen_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	arm64-v8a/libapplovin- native-crash-reporter.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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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: ['vsnprintf_chk', 'strlen_chk', 'memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86/libapplovin-native-crash- reporter.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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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: ['vsnprintf_chk', 'strlen_chk', 'memmove_chk']	False warning Symbols are available.

■ NIAP ANALYSIS v1.3

NO IDE	ENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
--------	----------	-------------	---------	-------------

SECOND SECOND PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/24	android.permission.READ_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_WIFI_STATE, android.permission.WRITE_EXTERNAL_STORAGE
Other Common Permissions	4/45	com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, 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	COUNTRY/REGION
-----------------------	--------	----------------

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
--------	--------	-------------

DOMAIN	STATUS	GEOLOCATION
vidtube.one	ok	IP: 188.114.97.6 Country: Spain Region: Madrid, Comunidad de City: Madrid Latitude: 40.416500 Longitude: -3.702560 View: Google Map
infoevent.startappservice.com	ok	IP: 213.35.117.150 Country: United Kingdom of Great Britain and Northern Ireland Region: England City: London Latitude: 51.508530 Longitude: -0.125740 View: Google Map
a.applovin.com	ok	No Geolocation information available.
schemas.applovin.com	ok	No Geolocation information available.
rt.applvn.com	ok	IP: 104.17.1.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.animewitcher.com	ok	IP: 34.149.87.45 Country: United States of America Region: Texas City: Houston Latitude: 29.941401 Longitude: -95.344498 View: Google Map
rt.applovin.com	ok	No Geolocation information available.
cdn.myanimelist.net	ok	IP: 18.164.68.24 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
support.start.io	ok	IP: 216.198.53.1 Country: United States of America Region: California City: San Francisco Latitude: 37.773968 Longitude: -122.410446 View: Google Map
0.0.0.0	ok	IP: 0.0.0.0 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map

DOMAIN	STATUS	GEOLOCATION
info.startappservice.com	ok	IP: 68.232.34.193 Country: United States of America Region: New Jersey City: Newark Latitude: 40.735661 Longitude: -74.172371 View: Google Map
myanimelist.net	ok	IP: 18.172.153.75 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
schemas.microsoft.com	ok	IP: 13.107.246.63 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
a.applvn.com	ok	IP: 104.17.1.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
compliance.iabtechnologylab.com	ok	IP: 188.114.97.6 Country: Spain Region: Madrid, Comunidad de City: Madrid Latitude: 40.416500 Longitude: -3.702560 View: Google Map
ms.applvn.com	ok	IP: 104.17.2.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
d.applvn.com	ok	IP: 104.17.1.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
adsmetadata.mobileadexchange.net	ok	IP: 213.35.101.181 Country: United States of America Region: Kentucky City: London Latitude: 37.128979 Longitude: -84.083260 View: Google Map

DOMAIN	STATUS	GEOLOCATION
d.applovin.com	ok	IP: 34.110.179.88 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
developer.android.com	ok	IP: 142.250.181.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
geoip.api.p3insight.de	ok	No Geolocation information available.
d26xw8rp6mlgfg.cloudfront.net	ok	IP: 18.64.142.129 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
req.startappservice.com	ok	IP: 213.35.101.181 Country: United States of America Region: Kentucky City: London Latitude: 37.128979 Longitude: -84.083260 View: Google Map

DOMAIN	STATUS	GEOLOCATION
prod-a.applovin.comhttps	ok	No Geolocation information available.
lh6.ggpht.com	ok	IP: 142.250.201.129 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
adsmetadata.startappservice.com	ok	IP: 213.35.101.181 Country: United States of America Region: Kentucky City: London Latitude: 37.128979 Longitude: -84.083260 View: Google Map
daneden.me	ok	IP: 76.76.21.164 Country: United States of America Region: California City: Walnut Latitude: 34.015400 Longitude: -117.858223 View: Google Map
imp.startappservice.com	ok	IP: 138.2.110.152 Country: United States of America Region: California City: Belmont Latitude: 37.532440 Longitude: -122.248833 View: Google Map

DOMAIN	STATUS	GEOLOCATION
support.google.com	ok	IP: 142.250.185.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
api.onesignal.com	ok	IP: 104.16.160.145 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
img.youtube.com	ok	IP: 192.178.24.238 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.applovin.com	ok	IP: 141.193.213.20 Country: United States of America Region: Texas City: Austin Latitude: 30.271158 Longitude: -97.741699 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.youtube.com	ok	IP: 192.178.24.238 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.startapp.com	ok	IP: 3.231.126.119 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
exoplayer.dev	ok	IP: 185.199.108.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map
docs.applovin.com	ok	IP: 34.160.63.2 Country: United States of America Region: Texas City: Houston Latitude: 29.941401 Longitude: -95.344498 View: Google Map
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
opensource.org	ok	IP: 199.16.173.137 Country: United States of America Region: Texas City: San Antonio Latitude: 29.425426 Longitude: -98.489349 View: Google Map
api.taboola.com	ok	IP: 199.232.81.44 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
ms.applovin.com	ok	IP: 34.102.162.219 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
www.w3.org	ok	IP: 104.18.23.19 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
funnel-assets.startappservice.com	ok	IP: 68.232.34.193 Country: United States of America Region: New Jersey City: Newark Latitude: 40.735661 Longitude: -74.172371 View: Google Map
www.facebook.com	ok	IP: 157.240.227.35 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
d2to8y50b3n6dq.cloudfront.net	ok	IP: 3.161.104.73 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
play.google.com	ok	IP: 192.178.24.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.example.com	ok	IP: 93.184.215.14 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
ns.adobe.com	ok	No Geolocation information available.
dash.applovin.com	ok	IP: 34.110.214.170 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
assets.applovin.com	ok	IP: 34.120.175.182 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
monetization-support.applovin.com	ok	IP: 34.110.151.135 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
vid.applovin.com	ok	IP: 34.160.64.118 Country: United States of America Region: Texas City: Houston Latitude: 29.941401 Longitude: -95.344498 View: Google Map
developer.apple.com	ok	IP: 17.253.73.202 Country: Germany Region: Berlin City: Berlin Latitude: 52.524368 Longitude: 13.410530 View: Google Map
scar.unityads.unity3d.com	ok	IP: 34.128.182.103 Country: United States of America Region: Texas City: Houston Latitude: 29.941401 Longitude: -95.344498 View: Google Map

A TRACKERS

TRACKER	CATEGORIES	URL
AppLovin (MAX and SparkLabs)	Advertisement, Identification, Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/72

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
IAB Open Measurement	Advertisement, Identification	https://reports.exodus-privacy.eu.org/trackers/328
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193
Startapp	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/195
Unity3d Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/121

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "0000000000000000000000000000000000
"google_crash_reporting_api_key" : "AlzaSyAcbWRwfFNnCpoydDXlEALWnM_TYVcJOMU"
"google_api_key" : "AlzaSyAcbWRwfFNnCpoydDXlEALWnM_TYVcJOMU"
com/Vo9wbFH89BbDbWFhUezQZOGPKmfkJSAtIbVWk3QxPbvJwcR8I79EVul0aB41a
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
c682b8144a8dd52bc1ad63

POSSIBLE SECRETS
c103703e120ae8cc73c9248622f3cd1e
13432e34a32071d95a4a36ec54796f80
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166 43812574028291115057151
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
3bb5f869a176d624977695287f115e42
b2f7f966-d8cc-11e4-bed1-df8f05be55ba
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
115792089210356248762697446949407573530086143415290314195533631308867097853951
49f946663a8deb7054212b8adda248c6
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
68647976601306097149819007990813932172694353001433054093944634591855431833976553942450577463332171975329639963713633211138647686124403 80340372808892707005449
5e5398f0546d1d7afd62641edb14d82894f11ddc41bce363a0c8d0dac82c9c5a
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
3A757365722F72656C656173652D6B657973

POSSIBLE SECRETS

5eb5a37e-b458-11e3-ac11-000c2940e62c ddb0823e-c7f4-4aec-b10b-09867ba74f38 3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f 2F73797374656D2F6C69622F6C69627265666572656E63652D72696C2E736F b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef 9a04f079-9840-4286-ab92-e65be0885f95 39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643 HSrCHRtOan6wp2kwOIGJC1RDtuSrF2mWVbio2aBcMHX9KF3iTJ1lLSzCKP1ZSo5yNolPNw1kCTtWpxELFF4ah1 11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650 26c2b6726dc4f2582c68e361a74e2374 c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66 258EAFA5-E914-47DA-95CA-C5AB0DC85B11 470fa2b4ae81cd56ecbcda9735803434cec591fa 6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

POSSIBLE SECRETS

115792089210356248762697446949407573529996955224135760342422259061068512044369

5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

⋮≡ SCAN LOGS

Timestamp	Event	Error
2024-09-27 01:40:37	Generating Hashes	ОК
2024-09-27 01:40:37	Extracting APK	ОК
2024-09-27 01:40:37	Unzipping	OK
2024-09-27 01:40:38	Getting Hardcoded Certificates/Keystores	ОК
2024-09-27 01:40:42	Parsing AndroidManifest.xml	OK
2024-09-27 01:40:42	Parsing APK with androguard	OK

2024-09-27 01:40:43	Extracting Manifest Data	ОК
2024-09-27 01:40:43	Performing Static Analysis on: Anime Witcher (com.anime.witcher)	OK
2024-09-27 01:40:43	Fetching Details from Play Store: com.anime.witcher	OK
2024-09-27 01:40:44	Manifest Analysis Started	ОК
2024-09-27 01:40:44	Checking for Malware Permissions	ОК
2024-09-27 01:40:44	Fetching icon path	ОК
2024-09-27 01:40:44	Library Binary Analysis Started	ОК
2024-09-27 01:40:44	Analyzing lib/x86_64/libapplovin-native-crash-reporter.so	ОК
2024-09-27 01:40:45	Analyzing lib/armeabi-v7a/libapplovin-native-crash-reporter.so	ОК
2024-09-27 01:40:47	Analyzing lib/arm64-v8a/libapplovin-native-crash-reporter.so	OK
2024-09-27 01:40:49	Analyzing lib/x86/libapplovin-native-crash-reporter.so	ОК

2024-09-27 01:40:50	Analyzing apktool_out/lib/x86_64/libapplovin-native-crash-reporter.so	ОК
2024-09-27 01:40:52	Analyzing apktool_out/lib/armeabi-v7a/libapplovin-native-crash-reporter.so	ОК
2024-09-27 01:40:54	Analyzing apktool_out/lib/arm64-v8a/libapplovin-native-crash-reporter.so	ок
2024-09-27 01:40:56	Analyzing apktool_out/lib/x86/libapplovin-native-crash-reporter.so	ОК
2024-09-27 01:40:59	Reading Code Signing Certificate	ок
2024-09-27 01:41:00	Running APKiD 2.1.5	ОК
2024-09-27 01:41:21	Updating Trackers Database	ОК
2024-09-27 01:41:21	Detecting Trackers	ОК
2024-09-27 01:41:29	Decompiling APK to Java with jadx	ок
2024-09-27 01:42:49	Converting DEX to Smali	ок
2024-09-27 01:42:49	Code Analysis Started on - java_source	ОК

2024-09-27 01:44:01	Android SAST Completed	ОК
2024-09-27 01:44:01	Android API Analysis Started	ОК
2024-09-27 01:44:27	Android Permission Mapping Started	ОК
2024-09-27 01:45:09	Android Permission Mapping Completed	ОК
2024-09-27 01:45:12	Finished Code Analysis, Email and URL Extraction	ОК
2024-09-27 01:45:12	Extracting String data from APK	ОК
2024-09-27 01:45:13	Extracting String data from SO	ОК
2024-09-27 01:45:13	Extracting String data from Code	ОК
2024-09-27 01:45:13	Extracting String values and entropies from Code	ОК
2024-09-27 01:45:17	Performing Malware check on extracted domains	ОК
2024-09-27 01:45:42	Saving to Database	ОК

Report Generated by - MobSF v4.0.7

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.

© 2024 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.