MOBSF

ANDROID STATIC ANALYSIS REPORT

app_icon

Stardust (4.12.0)

File Name:	com.stardust.app_1745.apk
Package Name:	com.stardust.app
Scan Date:	Sept. 1, 2025, 10:01 a.m.

App Security Score: 48/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 6/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	41	4	1	1

FILE INFORMATION

File Name: com.stardust.app_1745.apk
Size: 61.21MB

MD5: 62f0a633718dc58029720323b413dfad
SHA1: 54dba6d9f040bcadfa57706f25258264f9c6413f
SHA256: d4384ca139e262b4065ebecf537148718bbbb4ae09cf5bd5c959cc5c09825666

APP INFORMATION

App Name: Stardust
Package Name: com.stardust.app
Main Activity: com.stardust.app.presentation.splash.SplashActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 4.12.0
Android Version Code: 1745

APP COMPONENTS

Activities: 38
Services: 17
Receivers: 16
Providers: 2
Exported Activities: 20
Exported Services: 3
Exported Receivers: 7
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-06-27 23:54:37+00:00
Valid To: 2052-06-27 23:54:37+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xa32d219c1d6038c01a825b7e01e6b60adc67d9cf
Hash Algorithm: sha256
md5: 71d3945d3ed0ec64168e887370da0f1e
sha1: f8765ca1c175351e1eda56201bc4eb32edf33d76
sha256: 5dbccd0cdf4b3a10a96693a83f0de96ec2ad646f98325f1383090830dda78d9a
sha512: b9845262eef5c5117598ee444614a38a375b873b394d85d661faa81e9f127f800e3f1cfe5e7fb2a8322be8a72297444859b4e8a520f67d36d3aa356e5e33bfbd
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: f9f709714e3f833e935b9acd73e6de32ac662dcec22e5848a0fb91beb89e7bc6
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.health.READ_MENSTRUATION	unknown	Unknown permission	Unknown permission from android reference
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.
com.stardust.app.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.stardust.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>62f0a633718dc58029720323b413dfad.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></tr>
<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
ro.hardware check
ro.kernel.qemu check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

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

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.stardust.app.presentation.splash.SplashActivity	Schemes: stardust.app://, https://, Hosts: open, stardustapp.app.link, stardustapp-alternate.app.link, stardustapp.test-app.link, stardustapp-alternate.test-app.link,
com.stardust.app.presentation.deeplink.DeepLinkActivity	Schemes: http://, https://, stardust.app://, Hosts: stardust.app, stardust-app.onelink.me, Paths: /rownd, /home, /friends, /partners,

NETWORK SECURITY

HIGH: 1 | WARNING: 0 | INFO: 0 | SECURE: 0

NO	SCOPE	SEVERITY	DESCRIPTION
1	thestardustapp.com stardust.app	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: 0 | WARNING: 32 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Activity (com.stardust.app.presentation.main.syncwithfriends.addfriend.AddFriendsCycleActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (com.stardust.app.presentation.main.syncwithfriends.sharecycle.ShareCycleActivity) 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.
5	Activity (com.stardust.app.presentation.paywall.PaywallActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity (com.stardust.app.presentation.paywall.redeem.RedeemCodeActivity) 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.stardust.app.presentation.pregnancy.birthtypes.BirthTypeActivity) 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.stardust.app.presentation.main.profiletab.cycledetail.PastCycleDetailActivity) 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.stardust.app.presentation.main.addsymptoms.AddSymptomsActivity) 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.stardust.app.presentation.main.bbt.edit.AddEditBbtActivity) 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
11	Activity (com.stardust.app.presentation.settings.pregnancy.endpregnancy.EndPregnancyActivity) 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.stardust.app.presentation.dataprivacy.DataPrivacyActivity) 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.stardust.app.presentation.settings.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.
14	Activity (com.stardust.app.presentation.main.bbt.BasalBodyTempActivity) 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.stardust.app.presentation.main.journal.JournalActivity) 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.stardust.app.presentation.main.cyclepedia.CyclepediaActivity) 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.stardust.app.presentation.deeplink.DeepLinkActivity) 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.stardust.app.presentation.main.healthconnect.privacy.PermissionsRationaleActivity) 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-Alias (com.stardust.app.ViewPermissionUsageActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.START_VIEW_PERMISSION_USAGE [android:exported=true]	warning	An Activity-Alias 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.
20	Service (androidx.health.platform.client.impl.sdkservice.HealthDataSdkService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
21	Broadcast Receiver (com.onesignal.notifications.receivers.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.
22	Activity (com.onesignal.notifications.activities.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.

NO	ISSUE	SEVERITY	DESCRIPTION
23	Broadcast Receiver (com.onesignal.notifications.receivers.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.
24	Broadcast Receiver (com.onesignal.notifications.receivers.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.
25	Broadcast Receiver (com.onesignal.notifications.receivers.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.
26	Activity (com.onesignal.notifications.activities.NotificationOpenedActivity) 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.onesignal.notifications.activities.NotificationOpenedActivityAndroid22AndOlder) 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	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.
29	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.
30	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.
31	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
32	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.
33	High Intent Priority (999) - {1} Hit(s) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 7 | INFO: 3 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A2/e.java B0/c.java B2/i.java B2/j.java C1/a.java C2/e.java C2/j.java D2/a.java E2/c.java E2/d.java E2/f.java E2/v.java E2/w.java F/e.java F1/c.java G1/a.java G2/i.java G3/d.java G4/b.java H2/c.java H2/g.java H2/n.java H2/o.java H2/s.java H2/x.java H3/a.java I0/b.java I1/b.java I4/a.java J1/C0233f.java J1/C0452f.java J1/G.java K0/a.java K3/g.java L2/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				L2/d.java L2/j.java N2/r.java N2/s.java N2/v.java N2/x.java N6/i.java P4/i.java P4/j.java P4/o.java Q1/K.java Q4/e.java R2/j.java R4/a.java U3/a.java U3/b.java U3/c.java V2/a.java Y2/b.java Z1/q.java Z1/s.java a4/C0390f.java a4/C0609f.java b3/i.java com/akexorcist/channels/ScreenshotDetectionDelegate$startScreenshotDetection$1.java com/akexorcist/screenshotdetection/ScreenshotDetectionDelegate$startScreenshotDetection$1.java com/appsflyer/AFLogger.java com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFd1eSDK.java com/appsflyer/internal/AFd1fSDK.java com/appsflyer/internal/AFd1kSDK.java com/appsflyer/internal/AFd1nSDK.java com/appsflyer/internal/AFd1oSDK.java com/appsflyer/internal/AFd1pSDK.java com/appsflyer/internal/AFd1sSDK.java com/appsflyer/internal/AFd1tSDK.java com/appsflyer/internal/AFd1uSDK.java com/appsflyer/internal/AFe1kSDK.java com/appsflyer/internal/AFe1rSDK.java com/appsflyer/internal/AFe1uSDK.java com/appsflyer/internal/AFf1bSDK.java com/appsflyer/internal/q.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/c.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/e.java com/bumptech/glide/load/engine/i.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/bitmap/a.java com/bumptech/glide/m.java com/bumptech/glide/n.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/bumptech/glide/request/SingleRequest.java com/mixpanel/android/mpmetrics/a.java com/mixpanel/android/mpmetrics/c.java com/onesignal/common/c.java com/onesignal/debug/internal/logging/Logging.java com/revenuecat/purchases/common/DefaultLogHandler.java com/stardust/app/StardustApplication.java com/stardust/app/presentation/widget/wheelView/OldWheelView.java com/stardust/app/util/AbstractC0296a.java com/stardust/app/util/AbstractC1310a.java com/stardust/app/util/V.java com/superwall/sdk/analytics/internal/TrackingLogic.java com/superwall/sdk/billing/GoogleBillingWrapper.java com/superwall/sdk/deprecated/PaywallMessagesKt.java com/superwall/sdk/logger/Loggable.java com/superwall/sdk/misc/CurrentActivityTracker.java com/superwall/sdk/models/serialization/AnyMapSerializer.java com/superwall/sdk/models/serialization/AnySerializer.java com/superwall/sdk/network/Network.java com/superwall/sdk/network/device/DeviceHelper.java com/superwall/sdk/network/session/CustomHttpUrlConnection.java com/superwall/sdk/paywall/presentation/rule_logic/expression_evaluator/ExpressionEvaluator$evaluateExpression$2.java com/superwall/sdk/paywall/presentation/rule_logic/expression_evaluator/ExpressionEvaluator.java com/superwall/sdk/paywall/presentation/rule_logic/expression_evaluator/LiquidExpressionEvaluatorParams.java com/superwall/sdk/paywall/request/PaywallRequestManager$getRawPaywall$2.java com/superwall/sdk/paywall/vc/web_view/PaywallMessageKt.java com/superwall/sdk/paywall/vc/web_view/SWWebView.java com/superwall/sdk/paywall/vc/web_view/messaging/PaywallMessageHandler$didLoadWebView$3.java com/superwall/sdk/paywall/vc/web_view/messaging/PaywallMessageHandler.java com/superwall/sdk/store/transactions/TransactionManager.java com/superwall/sdk/view/SWWebViewInterface.java defpackage/TemplateLogic.java e3/C1085a.java e3/C1367a.java e6/b.java f1/C1096c.java f1/C1390c.java f1/h.java g0/C1108D.java g0/C1425D.java g0/e.java g0/f.java g0/g.java g0/m.java g0/r.java g0/w.java g1/C1113a.java g1/C1430a.java g3/C1119b.java g3/C1436b.java g5/C0381b.java g5/C1447b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				gd/l.java h/AbstractC1135f.java h/AbstractC1463f.java h/LayoutInflaterFactory2C1137h.java h/LayoutInflaterFactory2C1465h.java h0/C1140a.java h0/C1468a.java h3/r.java h4/l.java h5/e.java hd/f.java i1/i.java io/rownd/android/RowndClient.java io/rownd/android/authenticators/passkeys/PasskeyAuthentication.java io/rownd/android/authenticators/passkeys/PasskeyRegistration$register$1.java io/rownd/android/authenticators/passkeys/PasskeyRegistration.java io/rownd/android/models/RowndConfig.java io/rownd/android/models/network/RowndAPIException.java io/rownd/android/models/network/SignInLinkApi.java io/rownd/android/models/network/z.java io/rownd/android/models/repos/AppConfigRepo$loadAppConfigAsync$1.java io/rownd/android/models/repos/AuthRepo$fetchTokenAsync$1.java io/rownd/android/models/repos/AuthRepo$refreshTokenAsync$1.java io/rownd/android/models/repos/StateRepo$setup$1.java io/rownd/android/models/repos/UserRepo$loadUserAsync$1.java io/rownd/android/util/DefaultHeadersInterceptor$intercept$1.java io/rownd/android/util/SignInWithGoogle$signIn$1.java io/rownd/android/util/SignInWithGoogle$signOut$1.java io/rownd/android/util/SignInWithGoogle.java io/rownd/android/util/j.java io/rownd/android/util/l.java io/rownd/android/views/HubComposableBottomSheet$Content$1$1.java io/rownd/android/views/RowndJavascriptInterface.java io/rownd/android/views/h.java io/rownd/android/views/i.java j0/g.java j0/l.java j4/d.java j4/e.java j4/f.java j4/g.java j4/i.java k0/d.java k0/f.java k0/g.java k0/l.java k4/c.java k4/d.java k4/e.java k4/f.java l4/c.java l4/d.java l4/f.java m/g.java m1/AbstractC1243a.java m1/AbstractC1872a.java m4/c.java n4/A.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				n4/C.java n4/C1283g.java n4/C1284h.java n4/C1290n.java n4/C1926A.java n4/C1933g.java n4/C1934h.java n4/C1940n.java n4/CallableC1291o.java n4/CallableC1941o.java n4/E.java n4/N.java n4/r.java n4/x.java n4/y.java n4/z.java o0/h.java o0/m.java o3/e.java o4/C1970d.java o4/C1973g.java o4/d.java o4/g.java o4/j.java o4/l.java org/slf4j/helpers/Util.java p0/e.java r4/C2104a.java r4/a.java s2/C1388c.java s2/C2134c.java s4/e.java s4/f.java t1/ApplicationC1397b.java t1/ApplicationC2155b.java t1/C1396a.java t1/C2154a.java t4/C2163d.java t4/d.java u4/C2213a.java u4/a.java u4/c.java u4/e.java u4/f.java w0/c.java w2/C1461a.java w2/C2270a.java x0/i.java x2/C1470d.java x2/C1471e.java x2/C2290d.java x2/C2291e.java z2/C1502c.java z2/C2345c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	A2/c.java A2/o.java J8/a.java K8/g.java Y1/d.java com/bumptech/glide/load/engine/g.java com/onesignal/inAppMessages/internal/display/impl/WebViewManager.java com/onesignal/notifications/bridges/OneSignalHmsEventBridge.java com/onesignal/notifications/internal/c.java com/onesignal/notifications/receivers/FCMBroadcastReceiver.java com/revenuecat/purchases/amazon/AmazonBillingKt.java com/revenuecat/purchases/amazon/AmazonCacheKt.java com/revenuecat/purchases/common/BackendKt.java com/revenuecat/purchases/common/caching/DeviceCache.java com/revenuecat/purchases/common/diagnostics/DiagnosticsEntry.java com/revenuecat/purchases/common/diagnostics/DiagnosticsSynchronizer.java com/revenuecat/purchases/common/diagnostics/DiagnosticsTracker.java com/revenuecat/purchases/common/offlineentitlements/ProductEntitlementMapping.java com/revenuecat/purchases/common/verification/DefaultSignatureVerifier.java com/revenuecat/purchases/common/verification/Signature.java com/revenuecat/purchases/strings/ConfigureStrings.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java com/stardust/app/domain/repository/partner/model/PartnerInfo.java com/stardust/app/domain/repository/user/model/User.java com/stardust/app/domain/repository/user_me/usecase/o.java com/stardust/app/presentation/main/profiletab/pregnancy/e.java com/superwall/sdk/debug/DebugViewControllerActivity.java com/superwall/sdk/models/triggers/TriggerRuleOccurrence.java com/superwall/sdk/paywall/vc/SuperwallPaywallActivity.java com/superwall/sdk/paywall/vc/web_view/templating/models/DeviceTemplate.java d8/C0338g.java d8/C1350g.java h6/C0393a.java h6/C1519a.java io/rownd/android/models/RowndConfig.java io/rownd/android/views/HubBottomSheetBundleKeys.java k6/C0470e.java k6/C1627e.java w8/f.java y2/C1486c.java y2/C2319c.java
3	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/sun/jna/Native.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	gd/g.java gd/h.java gd/k.java gd/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	I4/a.java com/appsflyer/internal/AFb1zSDK.java com/revenuecat/purchases/common/UtilsKt.java
6	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	Cb/f.java P4/o.java com/onesignal/common/AndroidUtils.java ec/AbstractC0354a.java ec/AbstractC1378a.java ec/C0355b.java ec/C1379b.java fc/C0379a.java fc/C1420a.java io/opentelemetry/sdk/internal/AndroidFriendlyRandomHolder.java io/opentelemetry/sdk/internal/a.java io/opentelemetry/sdk/trace/RandomIdGenerator.java io/opentelemetry/sdk/trace/a.java
7	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/onesignal/inAppMessages/internal/display/impl/WebViewManager.java com/superwall/sdk/paywall/vc/web_view/SWWebView.java com/superwall/sdk/view/SWWebViewOld.java io/rownd/android/views/RowndWebView.java
8	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/onesignal/inAppMessages/internal/display/impl/WebViewManager.java com/superwall/sdk/view/SWWebViewOld.java io/rownd/android/views/RowndWebView.java
9	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	c4/C0994b.java c4/C1235b.java com/mixpanel/android/mpmetrics/MPDbAdapter.java com/onesignal/session/internal/outcomes/impl/j.java h3/r.java h3/t.java h3/u.java h3/v.java h3/w.java h3/x.java h3/y.java r5/c.java
10	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/superwall/sdk/storage/SearchPathDirectory.java io/rownd/android/RowndClient.java
11	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	io/rownd/android/models/network/SignInLinkApi.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/AFb1zSDK.java com/superwall/sdk/storage/CacheKeysKt.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	E2/h.java I0/b.java Q4/e.java com/airbnb/lottie/compose/h.java com/appsflyer/internal/AFa1jSDK.java com/appsflyer/internal/AFe1uSDK.java com/bumptech/glide/load/resource/bitmap/b.java com/revenuecat/purchases/common/FileHelper.java g0/g.java h2/CallableC1170j.java h2/CallableC1498j.java io/rownd/android/models/repos/GlobalStateSerializer.java k0/l.java md/u.java o4/C1973g.java o4/g.java q2/C1340d.java q2/C2050d.java s4/e.java u4/C2213a.java u4/a.java w2/C1461a.java w2/C1462b.java w2/C2270a.java w2/C2271b.java z1/C1494c.java z1/C2337c.java
00022	Open a file from given absolute path of the file	file	coil/disk/a.java com/appsflyer/internal/AFe1uSDK.java com/sun/jna/Native.java com/sun/jna/NativeLibrary.java com/superwall/sdk/storage/Storable.java h2/CallableC1170j.java h2/CallableC1498j.java o4/C1973g.java o4/g.java q2/C1340d.java q2/C2050d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	Y2/b.java com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFc1mSDK.java com/appsflyer/internal/AFc1rSDK.java com/revenuecat/purchases/common/HTTPClient.java com/superwall/sdk/network/Endpoint$makeRequest$2.java h5/c.java io/ktor/client/engine/android/AndroidClientEngine.java q2/C1338b.java q2/C2048b.java
00079	Hide the current app's icon	evasion	Z1/q.java h/LayoutInflaterFactory2C1137h.java h/LayoutInflaterFactory2C1465h.java
00147	Get the time of current location	collection location	h/LayoutInflaterFactory2C1137h.java h/LayoutInflaterFactory2C1465h.java
00075	Get location of the device	collection location	h/LayoutInflaterFactory2C1137h.java h/LayoutInflaterFactory2C1465h.java
00115	Get last known location of the device	collection location	h/LayoutInflaterFactory2C1137h.java h/LayoutInflaterFactory2C1465h.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	H5/b.java com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFb1uSDK.java com/appsflyer/internal/AFd1oSDK.java com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/b.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/OPPOHomeBader.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SonyHomeBadger.java com/stardust/app/presentation/auth/AuthActivity.java com/stardust/app/presentation/settings/paywall/ManageSubscriptionFragment.java com/stardust/app/util/C0318x.java com/stardust/app/util/C1332x.java com/stardust/app/util/IntentUtil$openGooglePlayStore$2.java com/superwall/sdk/paywall/vc/PaywallViewController.java io/rownd/android/views/i.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFf1gSDK.java com/appsflyer/internal/AFf1iSDK.java com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/b.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/EverythingMeHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/HuaweiHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/NovaHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/OPPOHomeBader.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SonyHomeBadger.java d2/e.java k6/C0470e.java k6/C1627e.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFa1eSDK.java com/appsflyer/internal/AFf1gSDK.java com/appsflyer/internal/AFf1hSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java z2/C1502c.java z2/C2345c.java
00089	Connect to a URL and receive input stream from the server	command network	Y2/b.java com/appsflyer/internal/AFc1mSDK.java com/appsflyer/internal/AFc1rSDK.java com/bumptech/glide/load/data/j.java com/revenuecat/purchases/common/HTTPClient.java h5/c.java
00109	Connect to a URL and get the response code	network command	Y2/b.java com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFc1mSDK.java com/appsflyer/internal/AFc1rSDK.java com/appsflyer/internal/AFd1lSDK.java com/bumptech/glide/load/data/j.java com/revenuecat/purchases/common/HTTPClient.java h5/c.java
00091	Retrieve data from broadcast	collection	com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFb1uSDK.java com/onesignal/core/activities/PermissionsActivity.java com/onesignal/notifications/receivers/FCMBroadcastReceiver.java k6/C0468c.java k6/C1625c.java u2/C1413E.java u2/C2187E.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/AFa1iSDK.java com/mixpanel/android/mpmetrics/a.java com/onesignal/common/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	H5/b.java com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/b.java com/stardust/app/presentation/auth/AuthActivity.java com/stardust/app/presentation/settings/paywall/ManageSubscriptionFragment.java com/stardust/app/util/C0318x.java com/stardust/app/util/C1332x.java com/superwall/sdk/paywall/vc/PaywallViewController.java
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1iSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFa1eSDK.java com/appsflyer/internal/AFf1gSDK.java com/appsflyer/internal/AFf1hSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java
00012	Read data and put it into a buffer stream	file	I0/b.java
00162	Create InetSocketAddress object and connecting to it	socket	gd/f.java gd/l.java
00163	Create new Socket and connecting to it	socket	gd/f.java gd/l.java
00189	Get the content of a SMS message	sms	R6/a.java com/appsflyer/internal/AFf1hSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java
00188	Get the address of a SMS message	sms	R6/a.java com/appsflyer/internal/AFf1hSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java
00200	Query data from the contact list	collection contact	R6/a.java com/appsflyer/internal/AFf1hSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java
00201	Query data from the call log	collection calllog	R6/a.java com/appsflyer/internal/AFf1hSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java
00125	Check if the given file path exist	file	h0/C1140a.java h0/C1468a.java j4/f.java
00094	Connect to a URL and read data from it	command network	h5/c.java r4/C2104a.java r4/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00108	Read the input stream from given URL	network command	h5/c.java
00121	Create a directory	file command	h0/C1140a.java h0/C1468a.java
00009	Put data in cursor to JSON object	file	com/mixpanel/android/mpmetrics/MPDbAdapter.java
00004	Get filename and put it to JSON object	file collection	com/mixpanel/android/mpmetrics/MPDbAdapter.java com/mixpanel/android/mpmetrics/a.java
00112	Get the date of the calendar event	collection calendar	com/stardust/app/presentation/onboarding/notificationpermission/NotificationPermissionViewModel.java com/stardust/app/util/C0301f.java com/stardust/app/util/C1315f.java
00014	Read file into a stream and put it into a JSON object	file	com/appsflyer/internal/AFe1uSDK.java o4/C1973g.java o4/g.java
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/AFe1uSDK.java o4/C1973g.java o4/g.java
00030	Connect to the remote server through the given URL	network	com/appsflyer/internal/AFa1uSDK.java com/bumptech/glide/load/data/j.java q2/C1338b.java q2/C2048b.java
00187	Query a URI and check the result	collection sms calllog calendar	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFa1eSDK.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://stardust-prod-5a598.firebaseio.com

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/442565757208/namespaces/firebase:fetch?key=AIzaSyDLkOVE0snA8yl5S2BHwlSJTZX42Wgznmo is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'castASpellOptions': '{"options":["Bring chocolate","Extra cuddles","Clean the house"]}', 'castASpellOptionsAndroid': '{"options":["Bring chocolate","Extra cuddles","Clean the house"]}', 'enableAgreements': 'false', 'enableAura': 'false', 'enableDailyDecode': 'false', 'enableDailyDecodeAndroid': 'true', 'enableDivineCreatorWitchType': 'true', 'enableEarthView': 'false', 'enableEnergyGraphs': 'false', 'enableFriendProfiles': 'true', 'enableFriendsAura': 'false', 'enablePaywall': 'true', 'enableReferral': 'true', 'enableReferralAndroid': 'true', 'enableSymptomIntensity': 'false', 'enableWearables': 'false', 'enable_superwall': 'true', 'onboardingOptimization': 'enabled', 'paywallHomeComponents': '{"freeComponents":["cycleForecast","partnerInvited","addYourPartner","yourPartnerList","currentPhase","energyAura","friendsEnergyCircle","earthView","currentMoon","crystalBall","onThisDay","galaxyBrain"],"paidComponents":["cycleForecast","partnerInvited","addYourPartner","yourPartnerList","currentPhase","energyAura","friendsEnergyCircle","earthView","currentMoon","crystalBall","onThisDay","galaxyBrain"]}', 'paywallHomeComponentsAndroid': '{"freeComponents":["cycleForecast","partnerInvited","addYourPartner","yourPartnerList","currentPhase","crystalBall","currentMoon","onThisDay","charity","galaxyBrain"],"paidComponents":["cycleForecast","partnerInvited","addYourPartner","yourPartnerList","currentPhase","crystalBall","currentMoon","onThisDay","charity","galaxyBrain"]}', 'paywallOptimization': 'Variant A', 'paywallProducts': '{"products":[{"isSelected":true,"id":"sd_4999_1m_1w"},{"isSelected":false,"id":"sd_3999_1y_1w"}]}', 'paywallProductsAndroid': '{"products":[{"isSelected":true,"id":"sd-0499-1m"},{"isSelected":false,"id":"sd-2499-1y"}]}', 'showLockOnCardsCyclepedia': 'false', 'showLockOnCardsDailyDecode': 'false', 'showLockOnCardsEnergy': 'false', 'useCaseErrorConfig': '{"UpdatePeriodLength":true,"LoadLogsData":false}'}, 'state': 'UPDATE', 'templateVersion': '167'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.CAMERA, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	4/44	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 MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
hub.rownd.io	ok	**IP:** 104.18.12.163 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.tiktok.com	ok	**IP:** 23.45.173.153 **Country:** United States of America **Region:** California **City:** El Segundo **Latitude:** 33.919182 **Longitude:** -118.416473 **View:** Google Map
appleid.apple.com	ok	**IP:** 17.157.64.68 **Country:** United States of America **Region:** California **City:** Cupertino **Latitude:** 37.316605 **Longitude:** -122.046486 **View:** Google Map
sinapps.s	ok	No Geolocation information available.
api.stardust.app	ok	**IP:** 35.82.95.9 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
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
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.74.110 **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.
simpression.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.
api.thestardustapp.com	ok	**IP:** 52.34.237.170 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
api.rownd.io	ok	**IP:** 104.18.13.163 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	**IP:** 159.100.250.151 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map
sattr.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
api.mixpanel.com	ok	**IP:** 35.190.25.25 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
rev.cat	ok	**IP:** 52.72.49.79 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
sregister.s	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.
ingest.us.signoz.cloud	ok	**IP:** 34.170.118.252 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
stardust.app	ok	**IP:** 18.155.173.111 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api-diagnostics.revenuecat.com	ok	**IP:** 54.88.247.37 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
scdn-stestsettings.s	ok	No Geolocation information available.
api.onesignal.com	ok	**IP:** 104.17.111.223 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
instagram.com	ok	**IP:** 31.13.70.174 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
sstats.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
ns.adobe.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
stardust-prod-5a598.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
sapp.s	ok	No Geolocation information available.
firebase-settings.crashlytics.com	ok	**IP:** 216.58.207.195 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
errors.rev.cat	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
docs.revenuecat.com	ok	**IP:** 18.238.109.116 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
app.rownd.io	ok	**IP:** 104.18.13.163 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
google.com	ok	**IP:** 216.58.207.206 **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.
api.revenuecat.com	ok	**IP:** 13.223.22.191 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

EMAILS

EMAIL	FILE
support@stardust.app	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
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	Analytics	https://reports.exodus-privacy.eu.org/trackers/118
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193
OpenTelemetry (OpenCensus, OpenTracing)	Analytics	https://reports.exodus-privacy.eu.org/trackers/412

HARDCODED SECRETS

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"com.google.firebase.crashlytics.mapping_file_id" : "2161fe3bf2074b28b2b0f581c07a007c"
"firebase_database_url" : "https://stardust-prod-5a598.firebaseio.com"
"google_api_key" : "AIzaSyDLkOVE0snA8yl5S2BHwlSJTZX42Wgznmo"
"google_crash_reporting_api_key" : "AIzaSyDLkOVE0snA8yl5S2BHwlSJTZX42Wgznmo"
701485d7d21614a919a4eb551ecea444
f4d0c973f2a83cb7d2cafcd0eada200a
470fa2b4ae81cd56ecbcda9735803434cec591fa
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
ae2044fb577e65ee8bb576ca48a2f06e
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
b6b8e7c0-fb66-4c6c-a391-bbf0a7d8dfcc
UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMlM=
XSgP8PMQggGTH79bXEB0321C6IdzBvqIt6
8b357f99d2524c6d3de00f39d1edcd54c7a201653167c3ad
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
c682b8144a8dd52bc1ad63
c9705c04-034c-44cc-af28-f76aa267bc5a
11f00dc53be30cfe213781d453297cf1

POSSIBLE SECRETS
c74ccde65819c710257c4575998266be
ee4655b3ec0d2ace448aa481008538b7
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
5181942b9ebc31ce68dacb56c16fd79f

PLAYSTORE INFORMATION

Title: Stardust: Period & Pregnancy

Score: 4.5816994 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.stardust.app

Developer Details: Stardust App Inc, Stardust+App+Inc, None, https://stardust.app/, support@stardust.app,

Release Date: Jun 27, 2022 **Privacy Policy:** Privacy link

Description:

Stardust is a free period, pregnancy, and hormone tracker health app that teaches you how to work with the phases of your cycle. We integrate science, ancient wisdom, astronomy and AI to help you understand the magic of your cycle, track your experiences, manifest goals, and befriend your body. Whether you are trying to predict your period or ovulation, get pregnant, track pregnancy, understand your symptoms, or just want to form a deeper connection to your body and see how your period syncs with the moon calendar, Stardust has you covered. • Get personal daily insights into your cycle and hormonal expertise • Predictions for your period, PMS symptoms, cravings, moods, and fertility • Cycle syncing and period tracking with your friends • Methods of leveraging lunar-menstrual synchronicity to manifest goals and nail it at life • Moon calendar and maps of the magic symbolism and folklore behind your cycle • Invite partners to stay in sync with your period and hormonal voyage • Better cycle tracking insights using sleep data NEW: If you're pregnant, you can now turn on Pregnancy Mode! • Daily affirmations for each trimester and symptom tracking • Weekly insights covering everything from diet and exercise to ancient wisdom • Hormone insights synced with the moon, and zodiac sign matchups between you and your baby Founded and led by women, we're committed to best-in-class privacy practices and will never sell or divulge your data. Find more information on how we protect you below. PRIVACY POLICY & TERMS OF SERVICE https://stardust.app/privacy-policy.html https://stardust.app/terms-of-use.html CONNECT WITH US Web - stardust.app Instagram - @stardust Tiktok - @stardust.app Note: Stardust should not be used as a birth control/contraception. The app does not substitute for professional medical advice, diagnosis, or treatment. Always seek the advice of a qualified healthcare provider. If you are having technical issues or have any questions about your cycle, we're here to help. Send an email to support@stardust.app

SCAN LOGS

Timestamp	Event	Error
2025-09-01 10:01:30	Generating Hashes	OK
2025-09-01 10:01:31	Extracting APK	OK
2025-09-01 10:01:31	Unzipping	OK
2025-09-01 10:01:42	Parsing APK with androguard	OK

2025-09-01 10:01:42	Extracting APK features using aapt/aapt2	OK
2025-09-01 10:01:42	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 10:01:45	Parsing AndroidManifest.xml	OK
2025-09-01 10:01:45	Extracting Manifest Data	OK
2025-09-01 10:01:45	Manifest Analysis Started	OK
2025-09-01 10:01:46	Reading Network Security config from network_security_config.xml	OK
2025-09-01 10:01:46	Parsing Network Security config	OK
2025-09-01 10:01:46	Performing Static Analysis on: Stardust (com.stardust.app)	OK
2025-09-01 10:01:47	Fetching Details from Play Store: com.stardust.app	OK
2025-09-01 10:01:49	Checking for Malware Permissions	OK
2025-09-01 10:01:49	Fetching icon path	OK
2025-09-01 10:01:49	Library Binary Analysis Started	OK
2025-09-01 10:01:49	Reading Code Signing Certificate	OK
2025-09-01 10:01:50	Running APKiD 2.1.5	OK

2025-09-01 10:01:55	Detecting Trackers	OK
2025-09-01 10:01:58	Decompiling APK to Java with JADX	OK
2025-09-01 10:02:22	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 10:02:22	Decompiling classes2.dex with JADX	OK
2025-09-01 10:02:32	Decompiling classes.dex with JADX	OK
2025-09-01 10:02:43	Decompiling classes2.dex with JADX	OK
2025-09-01 10:02:52	Decompiling classes.dex with JADX	OK
2025-09-01 10:03:02	Converting DEX to Smali	OK
2025-09-01 10:03:02	Code Analysis Started on - java_source	OK
2025-09-01 10:03:06	Android SBOM Analysis Completed	OK
2025-09-01 10:03:14	Android SAST Completed	OK
2025-09-01 10:03:14	Android API Analysis Started	OK
2025-09-01 10:03:23	Android API Analysis Completed	OK
2025-09-01 10:03:23	Android Permission Mapping Started	OK
2025-09-01 10:03:30	Android Permission Mapping Completed	OK

2025-09-01 10:03:31	Android Behaviour Analysis Started	OK
2025-09-01 10:03:41	Android Behaviour Analysis Completed	OK
2025-09-01 10:03:41	Extracting Emails and URLs from Source Code	OK
2025-09-01 10:03:46	Email and URL Extraction Completed	OK
2025-09-01 10:03:46	Extracting String data from APK	OK
2025-09-01 10:03:46	Extracting String data from Code	OK
2025-09-01 10:03:47	Extracting String values and entropies from Code	OK
2025-09-01 10:03:51	Performing Malware check on extracted domains	OK
2025-09-01 10:03:58	Saving to Database	OK

Report Generated by - MobSF v4.4.0

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.