ANDROID STATIC ANALYSIS REPORT

WeCare (1.47.5)

File Name:	com.sharecare.wecare_328.apk
Package Name:	com.sharecare.wecare
Scan Date:	Sept. 1, 2025, 8:37 a.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	24	2	2	1

FILE INFORMATION

File Name: com.sharecare.wecare_328.apk
Size: 21.12MB
MD5: d25c7ac38378b01b2b2e23cef1a5e164
SHA1: 45a2f2736a31964b660b9adddc63182e9990f652
SHA256: c6d5b71bc7f7dd73610319e3e3b41e7ca82856e0cf8a4ee1fca9960663ae3fb2

APP INFORMATION

App Name: WeCare
Package Name: com.sharecare.wecare
Main Activity: com.example.wecare_flutter.MainActivity
Target SDK: 33
Min SDK: 26
Max SDK:
Android Version Name: 1.47.5

Android Version Code: 328

APP COMPONENTS

Activities: 8
Services: 16
Receivers: 15
Providers: 4
Exported Activities: 3
Exported Services: 2
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: 2021-10-31 13:29:12+00:00
Valid To: 2051-10-31 13:29:12+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x8282feb640aa5796d23a4cbfd354d8e849dc19a3
Hash Algorithm: sha256
md5: 1debbff1cfa160a4a7f6057b8169e7b3
sha1: 6e927108c31297eaec0ba63fecf36014e8002e8b
sha256: b9660785f445f1c9928a01e809b986ac5f12b9a2e068d508f33807e364763272
sha512: 98c863a9bbc003df8a02c545ca517f6b2bb9a81535497898da143b36d4333781178bf104612ee59de2fbd273f0da55b4e2f8d136399929d5dda5e5a442273a27
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: f6711e009f0a6792fd6e2131ca1a5c588b0f317e8a5d609f0803115e7a463bef
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.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.ACCESS_MEDIA_LOCATION	dangerous	access any geographic locations	Allows an application to access any geographic locations persisted in the user's shared collection.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
com.sharecare.wecare.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.

PERMISSION	STATUS	INFO	DESCRIPTION
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.sharecare.wecare.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

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

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.example.wecare_flutter.MainActivity	Schemes: https://, sharecarewecare://, Hosts: @string/associated_domain, session, Path Prefixes: /landing.html,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **0** | INFO: **1**

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

MANIFEST ANALYSIS

HIGH: **0** | WARNING: **14** | 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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	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.
3	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.
4	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.
5	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.
6	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.
7	Activity (com.onesignal.NotificationOpenedReceiver) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
8	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.
9	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.
10	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
11	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
12	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
13	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.

NO	ISSUE	SEVERITY	DESCRIPTION
14	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: **2** | WARNING: **8** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/appsflyer/internal/d.java com/onesignal/OSUtils.java rb/a.java rb/b.java sb/a.java u6/c.java v3/p1.java w4/o0.java z4/b.java
2	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/flutter/plugin/editing/b.java io/flutter/plugin/platform/c.java
				a2/e.java a2/i.java a7/i1.java ab/a.java ab/b.java ab/c.java ai/doc/tensorio/core/modelbundle/AssetModelBundlesManager.java ai/doc/tensorio/core/modelbundle/Fil

NO	ISSUE	SEVERITY	STANDARDS	FILES
				eModelBundlesManager.java b2/a.java b3/b.java b6/b.java b6/d.java b6/e.java b6/i.java b6/j.java b6/s.java b6/u.java b6/v.java b8/b.java c0/a.java c2/c.java c2/d.java c2/f.java c2/s.java c2/t.java c6/d.java c6/g.java c6/h.java c6/k.java c6/r.java c6/v.java c8/c.java com/appsflyer/AFLogger.java com/baseflow/geolocator/GeolocatorLocationService.java com/baseflow/geolocator/b.java com/baseflow/geolocator/j.java com/baseflow/geolocator/m.java com/bugsnag/android/a0.java com/bugsnag/android/a1.java com/bumptech/glide/b.java com/lyokone/location/FlutterLocationService.java com/lyokone/location/a.java com/lyokone/location/b.java com/lyokone/location/c.java com/lyokone/location/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/onesignal/JobIntentService.java com/onesignal/c3.java com/onesignal/f.java com/onesignal/flutter/f.java com/wecare/health_metrics_observers/StepCountUpdateWorker.java com/wecare/health_metrics_observers/workouts/WorkoutTrackerWorker.java d3/a.java d3/d.java d6/j.java d9/f.java e0/a.java e2/a.java e6/m0.java f1/o.java f2/c.java f2/d.java f2/h.java f2/j.java f2/k.java f2/n.java f2/x.java f6/a.java f6/a1.java f6/c.java f6/d1.java f6/e0.java f6/e1.java f6/f1.java f6/h0.java f6/h1.java f6/l0.java f6/n1.java f6/q1.java f7/a.java f9/c.java f9/d.java g3/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				g7/a.java gd/b.java h0/c.java h1/d.java i6/a.java i9/a.java i9/i.java i9/s.java ia/s.java ia/u.java io/flutter/plugins/imagepicker/o.java io/flutter/plugins/webviewflutter/f.java io/flutter/plugins/webviewflutter/n3.java j2/a.java j2/d.java j2/j.java k3/k.java k6/a.java l/g.java l1/j.java l2/e.java l2/f.java l2/k.java l2/l.java l2/n.java l2/o.java l6/n.java l6/o.java m/c.java m0/c.java m1/b.java m2/d.java m3/a.java n7/c.java o1/a.java o1/n.java o1/o.java o1/p.java o2/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/tensorflow/lite/NativeInterpreterWrapper.java p0/a.java p7/g.java p7/n.java p9/b.java pc/c.java q6/z.java q8/a.java r5/r.java r6/c.java r9/b.java ra/a.java s1/b.java t1/a.java t2/a.java u0/k.java u1/d.java u1/e.java v2/b.java w1/b.java w1/j.java w1/l.java w2/a.java x1/c.java x1/e.java y1/h.java y1/i.java y1/k.java y1/q.java y1/z.java ya/h.java z1/i.java z1/j.java z5/g.java z6/z.java z8/c.java
4	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	b8/b.java com/appsflyer/internal/ae.java com/bugsnag/android/f0.java m9/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	d3/d.java ya/a.java ya/h.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	oc/c.java oc/d.java oc/g.java oc/h.java
7	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	b8/c.java ia/s.java io/flutter/plugins/imagepicker/l.java
8	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/onesignal/j3.java f9/c.java h1/g.java n0/a.java q3/b0.java q3/h0.java x8/k.java
9	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	c3/f.java com/bugsnag/android/v0.java com/onesignal/e4.java com/onesignal/h1.java com/onesignal/p1.java p1/d.java v1/g.java y1/d.java y1/p.java y1/x.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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/n4.java
11	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/n4.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/ae.java
13	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/bugsnag/android/RootDetector.java
14	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	b5/a.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/appsflyer/internal/ah.java com/bugsnag/android/NativeInterface.java com/bugsnag/android/e1.java com/bugsnag/android/ndk/NativeBridge.java com/bugsnag/android/o.java d3/d.java ia/j0.java ia/s.java io/flutter/plugins/imagepicker/l.java k0/a.java n0/b.java ya/h.java
00013	Read file and put it into a stream	file	ai/doc/tensorio/core/utilities/FileIO.java ai/doc/tensorio/tflite/model/TFLiteModel.java b8/c.java c2/f.java com/bugsnag/android/RootDetector.java com/bugsnag/android/k1.java com/bugsnag/android/u2.java com/bumptech/glide/load/a.java d3/a.java d3/d.java k0/c.java mb/i.java mb/k.java p1/f.java q5/g.java q5/h0.java t1/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00187	Query a URI and check the result	collection sms calllog calendar	b3/d.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java d3/a.java d3/d.java d3/e.java p9/b.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	b3/d.java com/appsflyer/internal/ag.java com/appsflyer/internal/cs.java com/appsflyer/internal/cu.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java d3/a.java d3/d.java d3/e.java p9/b.java x1/c.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/y.java com/onesignal/OSUtils.java h1/i.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	ab/b.java com/appsflyer/internal/ah.java com/appsflyer/internal/cw.java com/appsflyer/internal/i.java com/appsflyer/share/CrossPromotionHelper.java com/onesignal/OSUtils.java com/onesignal/d0.java com/onesignal/shortcutbadger/impl/SonyHomeBadger.java f6/t1.java g1/a.java io/flutter/plugins/imagepicker/l.java n1/a.java o1/a.java o1/n.java o1/p.java w2/a.java x2/a.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	ab/b.java com/onesignal/OSUtils.java com/onesignal/d0.java f6/t1.java n1/a.java o1/a.java o1/n.java o1/p.java w2/a.java x2/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/appsflyer/internal/ah.java com/appsflyer/internal/ao.java com/appsflyer/internal/cs.java com/appsflyer/share/CrossPromotionHelper.java com/onesignal/OSUtils.java com/onesignal/d0.java com/onesignal/shortcutbadger/impl/EverythingMeHomeBadger.java com/onesignal/shortcutbadger/impl/HuaweiHomeBadger.java com/onesignal/shortcutbadger/impl/NovaHomeBadger.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java com/onesignal/shortcutbadger/impl/SonyHomeBadger.java n1/a.java o1/a.java o1/n.java q5/h0.java
00091	Retrieve data from broadcast	collection	com/appsflyer/internal/ah.java com/appsflyer/internal/i.java com/onesignal/FCMBroadcastReceiver.java com/onesignal/PermissionsActivity.java com/onesignal/t1.java
00009	Put data in cursor to JSON object	file	com/onesignal/f0.java com/onesignal/i0.java com/onesignal/m0.java com/onesignal/r.java h1/g.java
00092	Send broadcast	command	com/onesignal/i0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	c8/c.java com/appsflyer/internal/ah.java com/appsflyer/internal/aj.java com/appsflyer/internal/bl.java com/appsflyer/internal/by.java com/onesignal/n3.java q5/s.java
00089	Connect to a URL and receive input stream from the server	command network	c8/c.java com/appsflyer/internal/ah.java com/appsflyer/internal/bl.java com/bugsnag/android/b0.java com/onesignal/n3.java q5/s.java w1/j.java
00030	Connect to the remote server through the given URL	network	com/appsflyer/internal/aj.java com/appsflyer/internal/by.java q5/s.java w1/j.java
00109	Connect to a URL and get the response code	network command	c8/c.java com/appsflyer/internal/ah.java com/appsflyer/internal/aj.java com/appsflyer/internal/bl.java com/appsflyer/internal/by.java com/appsflyer/internal/i.java com/appsflyer/share/CrossPromotionHelper.java com/bugsnag/android/b0.java com/onesignal/n3.java q5/s.java w1/j.java z5/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00094	Connect to a URL and read data from it	command network	q5/s.java
00108	Read the input stream from given URL	network command	q5/s.java
00189	Get the content of a SMS message	sms	b3/d.java com/appsflyer/internal/ag.java com/appsflyer/internal/cu.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java d3/e.java p9/b.java
00188	Get the address of a SMS message	sms	b3/d.java com/appsflyer/internal/ag.java com/appsflyer/internal/cu.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java d3/e.java p9/b.java
00053	Monitor data identified by a given content URI changes(SMS, MMS, etc.)	sms	b3/d.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	b3/d.java com/appsflyer/internal/ag.java com/appsflyer/internal/cs.java com/appsflyer/internal/cu.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00191	Get messages in the SMS inbox	sms	b3/d.java com/appsflyer/internal/ag.java com/appsflyer/internal/cu.java com/appsflyer/internal/cw.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00200	Query data from the contact list	collection contact	b3/d.java com/appsflyer/internal/ag.java com/appsflyer/internal/cu.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java d3/e.java p9/b.java
00201	Query data from the call log	collection calllog	b3/d.java com/appsflyer/internal/ag.java com/appsflyer/internal/cu.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java d3/e.java p9/b.java
00194	Set the audio source (MIC) and recorded file format	record	va/a.java
00197	Set the audio encoder and initialize the recorder	record	va/a.java
00196	Set the recorded file format and output path	record file	va/a.java
00161	Perform accessibility service action on accessibility node info	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/c.java
00137	Get last known location of the device	location collection	h1/i.java
00115	Get last known location of the device	collection location	h1/i.java
00132	Query The ISO country code	telephony collection	h1/i.java r5/m0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00199	Stop recording and release recording resources	record	ia/s.java
00028	Read file from assets directory	file	ai/doc/tensorio/core/utilities/AndroidAssets.java q5/c.java
00114	Create a secure socket connection to the proxy address	network command	kc/f.java
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/ah.java
00072	Write HTTP input stream into a file	command network file	com/appsflyer/internal/ah.java
00004	Get filename and put it to JSON object	file collection	com/appsflyer/internal/ah.java
00125	Check if the given file path exist	file	com/appsflyer/internal/ah.java
00153	Send binary data over HTTP	http	com/appsflyer/internal/ah.java
00016	Get location info of the device and put it to JSON object	location collection	com/appsflyer/internal/ah.java h1/c.java
00123	Save the response to JSON after connecting to the remote server	network command	com/appsflyer/internal/by.java
00023	Start another application from current application	reflection control	x2/a.java
00014	Read file into a stream and put it into a JSON object	file	b8/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00162	Create InetSocketAddress object and connecting to it	socket	oc/b.java oc/h.java
00163	Create new Socket and connecting to it	socket	oc/b.java oc/h.java
00147	Get the time of current location	collection location	com/lyokone/location/a.java
00202	Make a phone call	control	o1/p.java
00203	Put a phone number into an intent	control	o1/p.java
00209	Get pixels from the latest rendered image	collection	io/flutter/embedding/android/g.java
00210	Copy pixels from the latest rendered image into a Bitmap	collection	io/flutter/embedding/android/g.java
00193	Send a SMS message	sms	w2/a.java
00040	Send SMS	sms	w2/a.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.INTERNET, android.permission.READ_CONTACTS, android.permission.ACCESS_FINE_LOCATION, android.permission.READ_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.ACCESS_COARSE_LOCATION, android.permission.WAKE_LOCK, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	4/44	android.permission.ACTIVITY_RECOGNITION, com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
sinapps.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
api.amplitude.com	ok	**IP:** 44.234.5.97 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
cdn-settings.appsflyersdk.com	ok	**IP:** 18.238.109.119 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
plus.google.com	ok	**IP:** 216.58.211.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
notify.bugsnag.com	ok	**IP:** 35.186.205.6 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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.
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
sessions.bugsnag.com	ok	**IP:** 35.190.88.7 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
sconversions.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sgcdsdk.s	ok	No Geolocation information available.
exoplayer.dev	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
sattr.s	ok	No Geolocation information available.
bugsnag.com	ok	**IP:** 18.238.96.92 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
sars.s	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.
accounts.google.com	ok	**IP:** 209.85.233.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
profile-api.wecareapi.com	ok	**IP:** 34.199.129.178 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
api.onesignal.com	ok	**IP:** 104.17.111.223 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cdn-settings.segment.com	ok	**IP:** 18.238.93.145 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
developer.apple.com	ok	**IP:** 17.253.83.137 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **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.
schemas.microsoft.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cdn-testsettings.appsflyersdk.com	ok	**IP:** 18.155.174.188 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
docs.bugsnag.com	ok	**IP:** 18.155.173.77 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.googleapis.com	ok	**IP:** 216.58.207.234 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sapp.s	ok	No Geolocation information available.
dashif.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
svalidate.s	ok	No Geolocation information available.
aomedia.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

✉ EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	c6/q.java

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Bugsnag	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/207
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193

TRACKER	CATEGORIES	URL
Segment	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/62

HARDCODED SECRETS

POSSIBLE SECRETS
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
c682b8144a8dd52bc1ad63
c103703e120ae8cc73c9248622f3cd1e
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
9a04f079-9840-4286-ab92-e65be0885f95
5eb5a37e-b458-11e3-ac11-000c2940e62c
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1

POSSIBLE SECRETS
49f946663a8deb7054212b8adda248c6
b2f7f966-d8cc-11e4-bed1-df8f05be55ba
e2719d58-a985-b3c9-781a-b030af78d30e

PLAYSTORE INFORMATION

Title: WeCare by Sharecare

Score: 3.93 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.sharecare.wecare

Developer Details: Sharecare, Sharecare, None, https://www.wecaretravel.com/, support@wecaretravel.com,

Release Date: Feb 28, 2022 **Privacy Policy:** Privacy link

Description:

Introducing WeCare by Sharecare WeCare gives your team members a vacation spending account that significantly adds buying power to their personal travel. By doing so, WeCare modernizes health engagement with the ultimate incentive; travel and lifestyle experiences. Your team deserves a vacation spending account. Burnout is real. In this age of remote teams and work-from-home, team members are always connected. Taking proper time off to disconnect, reset and refresh is less likely despite the flexibility of WFH. Over $65 billion in PTO (paid time off) is left unused every year in the US alone. The US is really the “no vacation nation''. No wonder why workplace stress plays a role in $190 billion in healthcare spending according to an HBS research. An investment in your team’s vacation will have a direct impact on their mental and physical health - not to mention company culture and productivity. WeCare is the incentive platform for the new normal. Travel incentives go further. Our global partnerships with leading travel brands ensure that your team members get the best available rates at tens of thousands of hotels around the world. Your contributions to your team members’ VSA are immediately increased by 10% to ensure that travel incentives go further. In addition, members can earn up to 10% cash back when they book travel through WeCare. Every healthy action that they perform helps unlock additional cash back and gives them chances to win travel sweepstakes. Move more. Eat healthy. Travel safe. Your team members can earn more points on WeCare by making healthy choices or doing GeoHealth activities. Over 400k activities are available across the US including walking, running, cycling and hiking trails. Sharecare’s Community Well-Being Index (CWBI) powers WeCare’s AI to recommend activities. WeCare also recommends restaurants and cafe’s in any city around the world so that you can find healthy options wherever you are. Over 200k restaurants and cafes are recommended, not including fast-food restaurants. Finally, thousands of hotels and restaurants in WeCare are already Sharecare VERIFIED with Forbes Travel Guide so that you can dine and travel with confidence.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 08:37:15	Generating Hashes	OK
2025-09-01 08:37:15	Extracting APK	OK
2025-09-01 08:37:15	Unzipping	OK
2025-09-01 08:37:15	Parsing APK with androguard	OK
2025-09-01 08:37:15	Extracting APK features using aapt/aapt2	OK
2025-09-01 08:37:15	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 08:37:17	Parsing AndroidManifest.xml	OK
2025-09-01 08:37:17	Extracting Manifest Data	OK
2025-09-01 08:37:17	Manifest Analysis Started	OK

2025-09-01 08:37:17	Performing Static Analysis on: WeCare (com.sharecare.wecare)	OK
2025-09-01 08:37:18	Fetching Details from Play Store: com.sharecare.wecare	OK
2025-09-01 08:37:20	Checking for Malware Permissions	OK
2025-09-01 08:37:20	Fetching icon path	OK
2025-09-01 08:37:20	Library Binary Analysis Started	OK
2025-09-01 08:37:20	Reading Code Signing Certificate	OK
2025-09-01 08:37:20	Running APKiD 2.1.5	OK
2025-09-01 08:37:23	Detecting Trackers	OK
2025-09-01 08:37:24	Decompiling APK to Java with JADX	OK
2025-09-01 08:37:32	Converting DEX to Smali	OK
2025-09-01 08:37:32	Code Analysis Started on - java_source	OK

2025-09-01 08:37:34	Android SBOM Analysis Completed	OK
2025-09-01 08:37:37	Android SAST Completed	OK
2025-09-01 08:37:37	Android API Analysis Started	OK
2025-09-01 08:37:39	Android API Analysis Completed	OK
2025-09-01 08:37:39	Android Permission Mapping Started	OK
2025-09-01 08:37:42	Android Permission Mapping Completed	OK
2025-09-01 08:37:42	Android Behaviour Analysis Started	OK
2025-09-01 08:37:46	Android Behaviour Analysis Completed	OK
2025-09-01 08:37:46	Extracting Emails and URLs from Source Code	OK
2025-09-01 08:37:47	Email and URL Extraction Completed	OK
2025-09-01 08:37:47	Extracting String data from APK	OK

2025-09-01 08:37:47	Extracting String data from Code	OK
2025-09-01 08:37:47	Extracting String values and entropies from Code	OK
2025-09-01 08:37:48	Performing Malware check on extracted domains	OK
2025-09-01 08:37:50	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.