MOBSF

ANDROID STATIC ANALYSIS REPORT

ShutEye (1.6.6)

File Name:	health.sleep.sounds.tracker.alarm.calm_166.apk
Package Name:	health.sleep.sounds.tracker.alarm.calm
Scan Date:	Sept. 1, 2025, 1:34 p.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	20	2	3	1

FILE INFORMATION

File Name: health.sleep.sounds.tracker.alarm.calm_166.apk
Size: 113.38MB
MD5: e6e5166d30457d88a539d7ab8f7f72d1
SHA1: 8a2c315347cb14bbd134e0fd253b7c5345533fd6
SHA256: 332bddc974bcd7e66d7414f6a26e2792abc4bbeb813f7e6f35defd3de6352ca2

APP INFORMATION

App Name: ShutEye
Package Name: health.sleep.sounds.tracker.alarm.calm
Main Activity: life.enerjoy.sleep.SplashActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 1.6.6

Android Version Code: 166

APP COMPONENTS

Activities: 17
Services: 13
Receivers: 17
Providers: 8
Exported Activities: 2
Exported Services: 2
Exported Receivers: 5
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=HK, ST=HK, L=HK, O=Enerjoy, OU=Business, CN=Enerjoy
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-12-03 11:30:44+00:00
Valid To: 2119-11-09 11:30:44+00:00
Issuer: C=HK, ST=HK, L=HK, O=Enerjoy, OU=Business, CN=Enerjoy
Serial Number: 0x7c3ff50e
Hash Algorithm: sha256
md5: 5ab6ca0dbd93aad4fe9651e4940a340e
sha1: bfbea2cfe1f3e9abc3780f4d747aa85efe316235
sha256: 5d962fa108314b9edf866adfc17bb1121ffad4be74bd7e1d14cd8e6776a7aa60
sha512: 8e63aa07d51fea918f12b1665654af82bcbfa8035807786ba7acc3fef44e4203ca328601a0af8924da1e5dd3d17d441f5008d65b5089e0e49c6369c5cbdad4f0
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 842e9a0f6515e97dc643c677f7d852386d84c8bbd7a4e2d8d40bdeb893be8019
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	normal	enables foreground services for media playback.	Allows a regular application to use Service.startForeground with the type "mediaPlayback".
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.FOREGROUND_SERVICE_MICROPHONE	normal	permits foreground services with microphone use.	Allows a regular application to use Service.startForeground with the type "microphone".
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
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.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.
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.
health.sleep.sounds.tracker.alarm.calm.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	unknown	Unknown permission	Unknown permission from android reference
health.sleep.sounds.tracker.alarm.calm.permission.LE_FRAMEWORK	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>e6e5166d30457d88a539d7ab8f7f72d1.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>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.BRAND check
Build.DEVICE 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>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes2.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
life.enerjoy.sleep.MainActivity	Schemes: @string/fb_login_protocol_scheme://, app://, Hosts: health.sleep.sounds.tracker.alarm.calm,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.health.sleep.sounds.tracker.alarm.calm,

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: 10 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Activity (life.enerjoy.sleep.MainActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
3	Broadcast Receiver (life.enerjoy.sleep.main.profiler.sleep.BootReceiver) 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.
4	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
5	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.
6	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.
7	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
8	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.
9	Broadcast Receiver (com.appsflyer.SingleInstallBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Broadcast Receiver (com.appsflyer.MultipleInstallBroadcastReceiver) 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.

</> CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES

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	A5/C0011d.java A8/c.java A8/m.java A8/s.java B7/a.java F6/c.java G7/g.java L6/A1.java a2/t.java c2/E.java c2/K.java com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFb1gSDK.java d2/f.java d5/h.java f2/C1428a.java life/enerjoy/sleep/SleepApplication.java ma/AbstractC2025a.java ma/C2026b.java ma/C2027c.java n2/V.java na/C2130a.java v8/d.java z8/e.java z8/f.java
2	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	W3/x.java Ze/b.java
				A/g.java A4/A.java A4/C0007b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A4/e.java A4/q.java A4/q.java A4/t.java A4/u.java A4/v.java A4/y.java A5/D.java A5/G.java A8/j.java A8/q.java Af/m.java C4/d.java D4/c.java D4/d.java E8/Q.java F3/b.java F4/b.java G4/F.java G4/RunnableC0286a.java G4/k.java G4/l.java G4/o.java H4/g.java H4/h.java I4/d.java I7/a.java J1/g.java J4/c.java J7/b.java J7/c.java K4/C0369b.java K4/C0371d.java K4/z.java L1/c.java L3/g.java L6/C0383d0.java L6/CallableC0412r0.java L6/L.java L6/v1.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	L7/b.java M4/b.java M7/k.java M7/l.java M7/o.java M7/q.java M7/r.java M7/t.java M7/v.java M7/w.java Mb/d.java N3/c.java N4/B.java N4/C0460b.java N4/C0461c.java N4/H.java N4/i.java N4/m.java N4/p.java N4/r.java N4/v.java N6/a.java N7/g.java O6/m.java Qb/m.java R4/a.java R4/j.java R7/b.java Rb/d.java Rb/o.java S7/c.java V0/c.java V4/g.java W4/f.java W4/g.java X0/e.java X5/c.java Xc/d.java Z/a.java Ze/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				Ze/d.java Ze/e.java Ze/f.java a1/g.java c1/q.java com/appsflyer/internal/AFa1aSDK.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1uSDK.java com/appsflyer/internal/AFc1vSDK.java com/appsflyer/internal/AFf1cSDK.java com/appsflyer/internal/AFf1dSDK.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1kSDK.java com/appsflyer/internal/AFf1lSDK.java com/appsflyer/internal/AFf1tSDK.java com/appsflyer/internal/AFg1jSDK.java com/appsflyer/internal/AFg1nSDK.java com/appsflyer/share/CrossPromotionHelper.java com/appsflyer/share/LinkGenerator.java com/bumptech/glide/b.java com/bumptech/glide/e.java com/bumptech/glide/k.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/k.java com/bumptech/glide/m.java com/bumptech/glide/manager/l.java com/bumptech/glide/manager/m.java com/bumptech/glide/manager/p.java com/bumptech/glide/manager/q.java d8/C1362e.java f1/ServiceConnectionC1421A.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				f6/C1457c.java f6/h.java l5/l.java life/enerjoy/sleep/module/account/login/AccountLogoutFragment.java m5/AbstractC2017f.java nf/b.java q7/d.java q7/f.java r1/AbstractC2390a0.java r6/f.java r6/h.java t6/d.java t6/e.java u4/C2645b.java u6/BinderC2657H.java u6/HandlerC2656G.java uf/n.java vf/d.java x7/c.java
4	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	x8/d.java A5/D.java A8/j.java A8/q.java H/S.java H7/b.java L6/AbstractC0426y0.java L6/C0398k.java L6/J.java L6/v1.java Y1/b.java Y1/c.java a2/f.java a2/m.java d5/m.java f6/C1457c.java f6/h.java g6/k.java g6/l.java l2/C1898a.java o3/C2192b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	Ea/l.java Ia/d.java Ja/c.java Me/g.java Xe/a.java Zb/b.java bb/i.java ib/i.java uf/e.java uf/h.java uf/m.java uf/n.java
6	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	E4/h.java G4/C0291f.java G4/D.java G4/w.java I0/J.java R/C0537e0.java Sb/o.java X1/b.java d4/C1353b.java ed/e.java life/enerjoy/account/login/bean/EmailPasswordEntity.java vd/C2799a.java
7	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	M7/g.java q7/f.java
8	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	wd/o.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	A5/D.java M7/e.java g8/C1526c.java x7/b.java z6/b.java
10	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	L6/A1.java Xa/d.java l5/l.java u4/C2645b.java
11	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	A5/M.java L6/C0383d0.java c5/C1085i.java c5/M.java j5/i.java p5/C2275b.java
12	The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	Va/a.java
13	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/github/mikephil/charting/charts/Chart.java dc/C1369c.java r5/V.java vc/C2798e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
14	Calling Cipher.getInstance("AES") will return AES ECB mode by default. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	Mb/k.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	Xa/c.java Z1/o.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java f6/h.java s3/m.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	Ab/c.java Xa/c.java Z1/o.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java com/bumptech/glide/load/data/k.java f6/h.java h8/c.java
00109	Connect to a URL and get the response code	network command	F3/b.java L6/U.java Xa/c.java Z1/o.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java com/appsflyer/internal/AFf1jSDK.java com/bumptech/glide/load/data/k.java f6/h.java h8/c.java m6/C2019b.java p6/c.java r5/G.java
00030	Connect to the remote server through the given URL	network	L6/U.java Z1/o.java com/bumptech/glide/load/data/k.java s3/m.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	A5/C0011d.java A5/RunnableC0009b.java Ae/x.java Cc/B.java L6/A1.java L6/P0.java O7/n0.java Xa/c.java Z2/C0644a.java Z2/C0646c.java Z2/G.java Zd/e.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1bSDK.java com/appsflyer/internal/AFc1vSDK.java com/appsflyer/internal/AFf1vSDK.java com/bumptech/glide/d.java f9/AbstractC1469d.java lc/C1959n.java r5/K.java r5/O.java r5/V.java r5/X.java r6/f.java wb/h.java
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFi1bSDK.java com/appsflyer/internal/AFi1iSDK.java com/appsflyer/internal/AFi1jSDK.java r5/K.java r5/O.java
			A4/f.java A5/RunnableC0009b.java A8/d.java Af/u.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	B1/A.java B1/E.java C4/d.java C4/f.java D1/e.java E1/i.java Ie/d.java J1/g.java K4/z.java M7/g.java M7/k.java M7/o.java Mb/d.java N7/g.java Ne/b.java R7/a.java Z1/c.java Z1/u.java Ze/b.java c/C1043e.java c2/C1071z.java com/appsflyer/internal/AFb1iSDK.java com/appsflyer/internal/AFg1jSDK.java com/bumptech/glide/c.java d5/g.java e2/C1391g.java f1/AbstractC1427f.java g/AbstractC1479a.java ga/i.java h3/AbstractC1579c.java h3/C1584h.java k1/c.java k4/CallableC1827k.java l5/l.java mf/D.java p5/C2274a.java r5/C2435B.java u4/C2646c.java vc/C2798e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFi1bSDK.java r5/O.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFi1bSDK.java r5/O.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1bSDK.java r5/O.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFi1bSDK.java r5/O.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFi1bSDK.java r5/O.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1bSDK.java r5/O.java u4/C2646c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	A5/RunnableC0009b.java Lb/b.java O7/n0.java Xa/c.java Xa/d.java Xc/d.java Z1/u.java Z2/C0644a.java c4/C1073a.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFf1qSDK.java com/appsflyer/internal/AFi1iSDK.java com/appsflyer/internal/AFi1nSDK.java com/bumptech/glide/d.java f9/AbstractC1469d.java q0/c.java r5/K.java r5/V.java r5/c0.java r6/f.java
00012	Read data and put it into a buffer stream	file	A4/f.java J1/g.java d5/g.java l5/l.java r5/C2435B.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	Ae/x.java Z2/C0644a.java Z2/C0646c.java com/bumptech/glide/d.java r5/K.java r5/V.java r6/f.java wb/h.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	A4/A.java A5/Q.java H3/b.java L6/P0.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1vSDK.java r5/O.java
00014	Read file into a stream and put it into a JSON object	file	A5/RunnableC0009b.java N7/g.java Ze/b.java c2/C1071z.java com/appsflyer/internal/AFg1jSDK.java com/bumptech/glide/c.java d5/g.java p5/C2274a.java r5/C2435B.java u4/C2646c.java
00022	Open a file from given absolute path of the file	file	Ab/h.java B1/F.java N7/g.java bb/C1026b.java com/appsflyer/internal/AFg1jSDK.java com/github/mikephil/charting/charts/Chart.java g/AbstractC1479a.java k4/AbstractC1830n.java k4/CallableC1827k.java lb/d.java p3/C2272a.java r5/C2435B.java u4/C2646c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00005	Get absolute path of file and put it to JSON object	file	N7/g.java com/appsflyer/internal/AFg1jSDK.java r5/C2435B.java u4/C2646c.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1jSDK.java
00108	Read the input stream from given URL	network command	L6/S.java L6/S0.java Z1/o.java r5/K.java
00009	Put data in cursor to JSON object	file	bf/C1030a.java bf/C1032c.java bf/C1033d.java bf/C1035f.java d5/m.java u4/C2646c.java uf/l.java
00162	Create InetSocketAddress object and connecting to it	socket	uf/c.java uf/n.java
00163	Create new Socket and connecting to it	socket	uf/c.java uf/n.java
00147	Get the time of current location	collection location	q/C2336w.java
00075	Get location of the device	collection location	q/C2336w.java
00115	Get last known location of the device	collection location	q/C2336w.java
00187	Query a URI and check the result	collection sms calllog calendar	r5/O.java

RULE ID	BEHAVIOUR	LABEL	FILES
00010	Read sensitive data(SMS, CALLLOG) and put it into JSON object	sms calllog collection	u4/C2646c.java
00004	Get filename and put it to JSON object	file collection	L6/C0383d0.java d5/g.java d5/m.java r5/C2435B.java x7/a.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/AFi1xSDK.java r5/V.java
00028	Read file from assets directory	file	Z1/a.java
00132	Query The ISO country code	telephony collection	c/C1043e.java p2/C2269a.java
00015	Put buffer stream (data) to JSON object	file	r5/V.java
00171	Compare network operator with a string	network	r5/V.java
00094	Connect to a URL and read data from it	command network	Mb/d.java Z1/o.java r5/G.java
00065	Get the country code of the SIM card provider	collection	M6/b.java c/C1043e.java
00114	Create a secure socket connection to the proxy address	network command	qf/i.java

RULE ID	BEHAVIOUR	LABEL	FILES
00024	Write file after Base64 decoding	reflection file	k4/AbstractC1830n.java
00125	Check if the given file path exist	file	A5/RunnableC0009b.java
00112	Get the date of the calendar event	collection calendar	com/bumptech/glide/c.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/14802544971/namespaces/firebase:fetch?key=AIzaSyDHimznDGx27esNfJBJlkj3EUfT1RG8Y2U. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.RECEIVE_BOOT_COMPLETED, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.RECORD_AUDIO, android.permission.VIBRATE, android.permission.WAKE_LOCK
Other Common Permissions	3/44	android.permission.FOREGROUND_SERVICE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID

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
www.wwwwwwwwwwwboolean	ok	No Geolocation information available.
www.googleadservices.com	ok	**IP:** 142.250.74.162 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
graph-video.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
goo.gle	ok	**IP:** 67.199.248.13 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
sinapps.s	ok	No Geolocation information available.
enerjoy.life	ok	**IP:** 18.238.96.80 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
issuetracker.google.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

DOMAIN	STATUS	GEOLOCATION
.facebook.com	ok	No Geolocation information available.
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
www.wwwwwwwwwwwassetmanager	ok	No Geolocation information available.
graph.s	ok	No Geolocation information available.
default.url	ok	No Geolocation information available.
facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sdlsdk.s	ok	No Geolocation information available.
github.com	ok	**IP:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
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.
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
smonitorsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	**IP:** 142.250.74.68 **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.
www.wwwwvvww	ok	No Geolocation information available.
sattr.s	ok	No Geolocation information available.
www.wwwwwvwwwww	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
developers.facebook.com	ok	**IP:** 31.13.70.1 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
sars.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
app-measurement.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
www.wwwwwwwww	ok	No Geolocation information available.
pagead2.googlesyndication.com	ok	**IP:** 142.250.74.66 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
yaml.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
sregister.s	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
firebaseremoteconfigrealtime.googleapis.com	ok	**IP:** 142.250.74.170 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
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
firebaseinstallations.googleapis.com	ok	**IP:** 172.217.21.170 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
scdn-stestsettings.s	ok	No Geolocation information available.
testsolution.enerjoy.life	ok	**IP:** 44.217.83.125 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.wwwwvwwwpath2	ok	No Geolocation information available.
www.shuteye.ai	ok	**IP:** 34.225.123.59 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
aps-webhandler.appsflyer.com	ok	**IP:** 18.238.109.53 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.wwwvwwwww	ok	No Geolocation information available.
www.wwwwwvw	ok	No Geolocation information available.
shuteyeandroid.zendesk.com	ok	**IP:** 216.198.54.6 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.apple.com	ok	**IP:** 17.253.83.145 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
www.wwwvwwwwthis	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
svalidate-and-log.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
api.wellness.gympass.com	ok	**IP:** 18.238.109.15 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
cdn.enerjoy.life	ok	**IP:** 18.155.173.4 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **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
schemas.android.com	ok	No Geolocation information available.
sviap.s	ok	No Geolocation information available.

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
xmlpull.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
dashif.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
svalidate.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
shuteye.ai	ok	**IP:** 18.155.173.20 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
aomedia.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
console.firebase.google.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
goo.gl	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

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	r6/k.java
contact_sleep@enerjoy.life	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "becc3dab1e8e48a3a28ae431c255c763"

POSSIBLE SECRETS
"delete_account_password" : "Password"
"facebook_client_token" : "7448945be9602611d3f5884b2c2282e3"
"google_api_key" : "AIzaSyDHimznDGx27esNfJBJlkj3EUfT1RG8Y2U"
"google_crash_reporting_api_key" : "AIzaSyDHimznDGx27esNfJBJlkj3EUfT1RG8Y2U"
"com_facebook_device_auth_instructions" : "facebook.com/device□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"delete_account_password" : "Passwort"
"delete_account_password" : "Senha"
"com_facebook_device_auth_instructions" : "□□facebook.com/device□□□□□□□□□□□□□□"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
470fa2b4ae81cd56ecbcda9735803434cec591fa
49f946663a8deb7054212b8adda248c6
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
c56fb7d591ba6704df047fd98f535372fea00211

POSSIBLE SECRETS
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
9a04f079-9840-4286-ab92-e65be0885f95
9b8f518b086098de3d77736f9458a3d2f6f95a37
e2719d58-a985-b3c9-781a-b030af78d30e
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
d7b73ec8cf8f297218c1a65764f871a0
AUj/Yhio8H+C9j7rXYka0cCeF2p9JgnM2NiyqIctyiK0gHK6SDlJseS3tzRvWS9MWVVdY6iA2DIk5U04QDnSne32XBbP86XNGujO1cif5hu3NhD+GB4ETG9xAa0=
0f623429f3fefec1bdbb6deaaceb0262
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
f1968a47921a17415cd50e46b17da7db
cc2751449a350f668590264ed76692694a80308a
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
ffc830d0d484407eda20df0dd16bd820
c103703e120ae8cc73c9248622f3cd1e

POSSIBLE SECRETS
b6f31aa9a9ce3138c365d8adabbd25c7
c52ac91cd34073b9e64033c15ffbcdf0
4ddb0db97bbacfacf40f6a891f31c189
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
4f12eabf8096bee949b89b60fcb4e3d9

PLAYSTORE INFORMATION

Title: ShutEye®: Sleep Tracker

Score: 4.5511594 **Installs:** 5,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** health.sleep.sounds.tracker.alarm.calm

Developer Details: ENERJOY PTE. LTD., 5785833978814606982, None, https://enerjoy.life/, service_android@support.shuteye.ai,

Release Date: May 19, 2022 **Privacy Policy:** Privacy link

Description:

Embark on a journey into the realm of serene slumber and tranquility, guided by the captivating melodies of ShutEye's innovative sleep sounds. Welcome to the world of ShutEye: the ultimate sleep-tracking app that empowers you to take control of your sleep like never before. Elevate Your Sleep Quality: ShutEye is tailored to enhance your sleep quality. Amid its array of functionalities, the brilliance of the sleep sounds feature stands out, offering an auditory escape into dreamscapes crafted to whisk you away from daily stresses and guide you into restful slumber. Unveil Sleep Patterns: Uncover the mysteries of your sleep patterns and decode the intricate nuances influencing your sleep cycle with our state-of-the-art sleep-tracking technology. Our innovative sleep recorder enables you to capture moments of nighttime whispers and laughter, allowing you to share these cherished memories with loved ones. Wake Refreshed: Arise from slumber revitalized and invigorated with the groundbreaking alarm feature. Moreover, the snore detector keeps you informed about your sleep quality, ensuring you're always in the know about your nighttime habits. Universally Embracing: ShutEye is designed to be inclusive, catering to a diverse range of individuals seeking improved sleep quality. Craft your personalized symphony of white noise and nature's melodies to create a sleep environment that aligns perfectly with your preferences. Seize Better Sleep: The significance of quality sleep cannot be overstated. Don't let sleep troubles hinder your overall well-being. Seize the opportunity today to download the ShutEye sleep tracker and embark on your journey towards profound, rejuvenating rest, harmonized by the soothing embrace of sleep sounds. Embrace Sweet Dreams: With the promise of sweet dreams and a brighter tomorrow, it's time to embrace a new chapter of restful sleep. Allow the symphony of ShutEye's sleep sounds to guide you into tranquil slumber and experience the

transformation firsthand. Welcome to a world where your sleep takes center stage. Welcome to ShutEye. ShutEye is registered trademark of Enerjoy. (Reg. No.6463393)

SCAN LOGS

Timestamp	Event	Error
2025-09-01 13:34:04	Generating Hashes	OK
2025-09-01 13:34:04	Extracting APK	OK
2025-09-01 13:34:04	Unzipping	OK
2025-09-01 13:34:05	Parsing APK with androguard	OK
2025-09-01 13:34:05	Extracting APK features using aapt/aapt2	OK
2025-09-01 13:34:05	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 13:34:07	Parsing AndroidManifest.xml	OK
2025-09-01 13:34:07	Extracting Manifest Data	OK

2025-09-01 13:34:07	Manifest Analysis Started	OK
2025-09-01 13:34:07	Performing Static Analysis on: ShutEye (health.sleep.sounds.tracker.alarm.calm)	OK
2025-09-01 13:34:09	Fetching Details from Play Store: health.sleep.sounds.tracker.alarm.calm	OK
2025-09-01 13:34:10	Checking for Malware Permissions	OK
2025-09-01 13:34:10	Fetching icon path	OK
2025-09-01 13:34:10	Library Binary Analysis Started	OK
2025-09-01 13:34:11	Reading Code Signing Certificate	OK
2025-09-01 13:34:11	Running APKiD 2.1.5	OK
2025-09-01 13:34:15	Detecting Trackers	OK
2025-09-01 13:34:16	Decompiling APK to Java with JADX	OK
2025-09-01 13:34:30	Converting DEX to Smali	OK

2025-09-01 13:34:30	Code Analysis Started on - java_source	OK
2025-09-01 13:34:33	Android SBOM Analysis Completed	OK
2025-09-01 13:34:41	Android SAST Completed	OK
2025-09-01 13:34:41	Android API Analysis Started	OK
2025-09-01 13:34:49	Android API Analysis Completed	OK
2025-09-01 13:34:50	Android Permission Mapping Started	OK
2025-09-01 13:34:55	Android Permission Mapping Completed	OK
2025-09-01 13:34:55	Android Behaviour Analysis Started	OK
2025-09-01 13:35:05	Android Behaviour Analysis Completed	OK
2025-09-01 13:35:05	Extracting Emails and URLs from Source Code	OK
2025-09-01 13:35:09	Email and URL Extraction Completed	OK

2025-09-01 13:35:09	Extracting String data from APK	OK
2025-09-01 13:35:10	Extracting String data from Code	OK
2025-09-01 13:35:10	Extracting String values and entropies from Code	OK
2025-09-01 13:35:13	Performing Malware check on extracted domains	OK
2025-09-01 13:35:16	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.