ANDROID STATIC ANALYSIS REPORT

Deep Sleep Sounds (1.9.0)

File Name:	com.kitefaster.whitenoise_308.apk
Package Name:	com.kitefaster.whitenoise
Scan Date:	Aug. 30, 2025, 10:35 p.m.

App Security Score:	51/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	5/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	22	2	2	1

FILE INFORMATION

File Name: com.kitefaster.whitenoise_308.apk
Size: 53.39MB
MD5: c74435d686827d2add7e5f086a3f4aa2
SHA1: 2153dada50cc6376c0a6e49760247fc8381f1f3f
SHA256: 19b43ed26cfa3fe883e165441fa73dea876dabecb69e1a194a0ee76a5af74d28

APP INFORMATION

App Name: Deep Sleep Sounds
Package Name: com.kitefaster.whitenoise
Main Activity: com.kitefaster.whitenoise.MainActivity
Target SDK: 34
Min SDK: 22
Max SDK:
Android Version Name: 1.9.0
Android Version Code: 308

APP COMPONENTS

Activities: 19
Services: 13
Receivers: 14
Providers: 4
Exported Activities: 6
Exported Services: 1
Exported Receivers: 5
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-04-03 19:07:43+00:00
Valid To: 2048-04-03 19:07:43+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xb4c939b1cdf7d3d62ba40020d7d27f3cf72fe82f
Hash Algorithm: sha256
md5: 0497ba01bd6163348f5911d722921b4b
sha1: a7b676b52f8d3d924f2ae0346be6a3daa0c051a8

sha256: afeb1875939f36afe471bd3fc732b5a97dd1a9bc545af3fc5354e67ba6312261
sha512: e17651413da277f5826687e8375bbc147d1619db306d0d1ece88960818c16df2b0da448ece7b24d2b10385b2381773359993d0341e7a9d01a304a4858cc95c16
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: fc8a43d18067b4ef5def0d05c1c06f5e5d2a44db96237f8fe13fa11489aa5141
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_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	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.

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.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.kitefaster.whitenoise.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>c74435d686827d2add7e5f086a3f4aa2.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>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator check
network operator name check
ro.kernel.qemu check
possible ro.secure check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
<tr><td>classes2.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.kitefaster.whitenoise.MainActivity	Schemes: https://, deepsleepsounds://, com.deepsleepsounds://, Hosts: deepsleepsounds.onelink.me, deepsleepsounds.com, get.deepsleepsounds.com, Path Prefixes: /U0RY,

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

🔒 NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

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

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **12** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.1-5.1.1, [minSdk=22]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Broadcast Receiver (com.kitefaster.whitenoise.data.SoundsUpdater$LanguageUpdateReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Broadcast Receiver (com.kitefaster.whitenoise.application.SoundControlReceiver) 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.google.firebase.auth.internal.GenericIdpActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Activity (com.google.firebase.auth.internal.RecaptchaActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	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.
7	Activity (androidx.core.google.shortcuts.TrampolineActivity) 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	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.
9	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.
10	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) 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 (androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity) 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
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.

</> CODE ANALYSIS

HIGH: **0** | WARNING: **7** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/g.java ac/j.java ao/c.java b7/h.java ba/b.java ba/c.java ba/e.java ba/i.java ba/j.java ba/l.java ba/m.java c0/d.java c4/e.java c4/i0.java c5/h.java ca/f.java ca/i.java ca/n.java ca/r.java ca/u.java cc/c.java cc/u.java cf/m.java cf/x.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/AFg1hSDK.java com/appsflyer/internal/AFg1jSDK.java com/appsflyer/internal/AFg1nSDK.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/appsflyer/share/CrossPromotionHelper.java com/appsflyer/share/LinkGenerator.java com/bugsnag/android/c1.java com/bugsnag/android/e1.java com/bugsnag/android/k0.java com/bugsnag/android/y.java com/bumptech/glide/b.java com/bumptech/glide/c.java com/bumptech/glide/d.java com/bumptech/glide/load/data/l.java com/kitefaster/whitenoise/MainActivity.java com/kitefaster/whitenoise/audio/DeepSleepSoundsPlayer.java com/kitefaster/whitenoise/downloader/DownloadWorker.java com/kitefaster/whitenoise/views/controls/ControlsFragment.java com/revenuecat/purchases/common/DefaultLogHandler.java d5/q.java e/c.java e0/e.java e1/r.java e4/q.java e4/y.java f9/g.java f9/o2.java fa/a.java fb/b.java fg/l.java g4/j.java g4/k.java gh/o.java h0/f.java h0/i.java h0/m.java h1/e.java h2/l.java h7/u0.java ha/e.java i/e.java i/f.java i9/o0.java i9/s.java id/a0.java id/m.java id/s.java ie/s.java ig/w.java ig/y.java j/a0.java j/h.java j/j0.java j/q.java j6/c.java j9/g.java jg/b.java jg/c.java k6/e.java ka/c.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	kd/d.java kf/c.java l0/f.java l0/j0.java lb/b.java ld/c.java lg/c.java lg/u.java m2/r.java m6/c.java md/d.java n6/g0.java n6/l.java n6/m.java n6/p.java nc/d.java nd/c.java o/h0.java o0/q.java o1/t.java o6/h.java o6/i.java oa/o4.java p001if/c.java p2/b.java p5/g0.java p5/h.java p5/t.java p6/j.java pd/g.java pd/k.java pd/l.java pd/n.java pd/p.java pd/r.java pd/s.java pd/t.java pd/u.java q0/i.java q0/j.java q0/k.java q1/b.java q5/h0.java q5/i0.java q5/p.java qa/a.java qd/l.java qf/k0.java qf/o.java r0/c.java r1/c.java r1/g.java r4/g0.java r4/h1.java r4/n1.java r5/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				r5/a.java r6/l.java r8/c.java r8/h.java rn/c.java s4/k.java s4/v.java sa/a.java sf/d.java sf/e.java t/o.java t1/a.java t1/b1.java t1/c.java t1/c0.java t1/e.java t1/f.java t1/f1.java t1/h.java t1/i.java t1/i0.java t1/l.java t1/m.java t1/m0.java t1/m1.java t1/n.java t1/o.java t1/q.java t1/r0.java t1/t.java t1/u1.java t1/v.java t1/w1.java t1/x1.java t1/y0.java t1/z1.java t6/b.java t7/g.java ta/a.java td/b.java u/a3.java u/k.java u/k2.java u/o0.java u/p3.java u/q2.java u/t2.java u1/c.java u5/g.java u6/b.java u6/c.java u6/o.java u6/q.java u6/z.java ub/a.java uc/g.java un/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				un/a.java vd/b.java w6/a.java w6/g.java wg/b.java wm/m.java x4/g.java xm/d.java y0/a1.java y0/b.java y0/d2.java y0/s.java y5/o.java y5/v.java y6/r.java zb/e.java
2	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/e.java c5/h.java ie/s.java ke/e0.java ke/k0.java ke/l0.java ke/n0.java m2/g.java m2/k.java oa/j4.java oa/k.java oa/l8.java oa/x7.java p5/k0.java r8/c.java r8/h.java s8/h.java s8/i.java s8/o.java uc/d.java x4/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/AFa1uSDK.java com/appsflyer/internal/AFb1gSDK.java com/appsflyer/internal/AFc1fSDK.java e2/h.java f9/r.java gj/a.java gj/b.java gj/c.java hj/a.java j/q.java jh/g1.java jh/g4.java jh/i1.java jh/t0.java jh/y2.java kh/n.java l2/o0.java m2/y.java oa/e8.java qh/u.java s2/a1.java xg/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	com/bugsnag/android/z.java com/revenuecat/purchases/common/UtilsKt.java ef/i.java ha/e.java jf/b.java pd/g.java td/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/bugsnag/android/w0.java com/revenuecat/purchases/amazon/AmazonBillingKt.java com/revenuecat/purchases/amazon/AmazonCacheKt.java com/revenuecat/purchases/common/BackendKt.java com/revenuecat/purchases/common/BackgroundAwareCallbackCacheKey.java com/revenuecat/purchases/common/caching/DeviceCache.java com/revenuecat/purchases/common/diagnostics/DiagnosticsEntry.java com/revenuecat/purchases/common/diagnostics/DiagnosticsHelper.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/SubscriberAttribute.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java fm/t0.java g6/g.java i2/a.java io/jsonwebtoken/JwsHeader.java je/a.java kh/k.java l6/l.java le/k.java me/h.java n6/e0.java n6/f.java n6/x.java oe/z.java x/b.java xn/e.java y5/d.java
6	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	cc/c.java com/bugsnag/android/RootDetector.java pd/g.java zb/e.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	uc/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	io/jsonwebtoken/impl/security/EcSignatureAlgorithm.java io/jsonwebtoken/impl/security/RsaSignatureAlgorithm.java
9	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	wm/d.java wm/g.java wm/k.java wm/m.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	f9/r.java l/j.java oa/e8.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	com/kitefaster/whitenoise/views/settings/FeatureTestingActivity.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	com/appsflyer/internal/AFg1jSDK.java i9/m.java qd/g.java uc/d.java vd/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	a2/e.java c5/h.java com/appsflyer/internal/AFg1jSDK.java com/bugsnag/android/NativeInterface.java com/bugsnag/android/j1.java com/kitefaster/whitenoise/downloader/DownloadWorker.java ef/l.java gh/o.java ig/g0.java j1/l0.java j1/r.java j1/z.java lg/j.java lg/t.java n0/f.java qd/g.java y4/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	aj/k.java com/appsflyer/internal/AFb1iSDK.java com/appsflyer/internal/AFg1jSDK.java com/bugsnag/android/RootDetector.java com/bugsnag/android/c1.java com/bugsnag/android/m1.java com/bugsnag/android/r0.java com/bugsnag/android/t1.java com/bumptech/glide/c.java com/revenuecat/purchases/common/FileHelper.java ef/l.java h7/u0.java i9/m.java j1/g0.java j1/l0.java j2/c.java j2/t.java j6/c.java j6/e.java l0/h.java l1/g.java l6/g.java m1/k.java p4/a.java p4/d.java p4/i.java pd/g.java pd/p.java q0/i.java q0/j.java qd/g.java r1/g.java td/a.java uc/d.java vd/b.java y5/l.java
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/AFg1jSDK.java n0/f.java qd/g.java
00089	Connect to a URL and receive input stream from the server	command network	com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java com/bugsnag/android/z.java com/bumptech/glide/load/data/l.java com/revenuecat/purchases/common/HTTPClient.java j2/o.java kf/c.java lg/o.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/l.java com/kitefaster/whitenoise/downloader/DownloadWorker.java j2/o.java
00109	Connect to a URL and get the response code	network command	c9/b.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java com/appsflyer/internal/AFf1jSDK.java com/bugsnag/android/z.java com/bumptech/glide/load/data/l.java com/kitefaster/whitenoise/downloader/DownloadWorker.java com/revenuecat/purchases/common/HTTPClient.java j2/o.java j9/i.java kf/c.java lg/o.java
00091	Retrieve data from broadcast	collection	com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1vSDK.java e6/m0.java i9/s.java i9/u0.java oa/o6.java s5/c.java
00012	Read data and put it into a buffer stream	file	r1/g.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	ah/b.java ba/h.java ca/f.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1bSDK.java com/appsflyer/internal/AFc1vSDK.java com/appsflyer/internal/AFf1vSDK.java com/bumptech/glide/c.java com/kitefaster/whitenoise/views/dialogue/paywall/OnboardingPaywallPage.java e4/b.java e4/d.java e9/i.java f9/g.java i9/r0.java ie/s.java ig/y.java n0/f.java oa/e8.java oa/o6.java rd/k1.java t1/m.java ue/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	ca/f.java com/bumptech/glide/c.java com/kitefaster/whitenoise/views/dialogue/paywall/OnboardingPaywallPage.java e4/b.java e4/d.java e9/i.java f9/g.java i9/r0.java ie/s.java ig/y.java
00009	Put data in cursor to JSON object	file	u0/a.java uc/d.java uf/v.java
00004	Get filename and put it to JSON object	file collection	n0/f.java td/b.java uc/d.java uf/v.java
00112	Get the date of the calendar event	collection calendar	com/bugsnag/android/d1.java com/fasterxml/jackson/databind/ser/std/n0.java e/c.java h8/x.java
00036	Get resource file from res/raw directory	reflection	ca/f.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFf1qSDK.java com/appsflyer/internal/AFi1iSDK.java com/appsflyer/internal/AFi1nSDK.java com/bumptech/glide/c.java e4/b.java i9/r0.java ie/s.java ig/y.java j2/t.java n0/f.java r6/l.java
00026	Method reflection	reflection	n0/f.java q5/h0.java yj/c0.java
00072	Write HTTP input stream into a file	command network file	lg/o.java
00094	Connect to a URL and read data from it	command network	j2/o.java lg/o.java t7/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00108	Read the input stream from given URL	network command	j2/o.java lg/o.java oa/r4.java oa/r6.java
00125	Check if the given file path exist	file	ef/l.java md/d.java td/b.java uf/v.java
00075	Get location of the device	collection location	y5/v.java
00137	Get last known location of the device	location collection	y5/v.java
00024	Write file after Base64 decoding	reflection file	p2/b.java
00034	Query the current data network type	collection network	i9/a.java
00162	Create InetSocketAddress object and connecting to it	socket	wm/c.java wm/m.java
00163	Create new Socket and connecting to it	socket	wm/c.java wm/m.java
00114	Create a secure socket connection to the proxy address	network command	sm/j.java
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFi1bSDK.java ka/c.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFi1bSDK.java ka/c.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFi1bSDK.java ka/c.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFi1bSDK.java ka/c.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1bSDK.java ka/c.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1jSDK.java

RULE ID	BEHAVIOUR	LABEL	FILES
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1bSDK.java
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFi1bSDK.java com/appsflyer/internal/AFi1iSDK.java com/appsflyer/internal/AFi1jSDK.java
00132	Query The ISO country code	telephony collection	v2/f.java
00121	Create a directory	file command	td/b.java uf/v.java
00104	Check if the given path is directory	file	td/b.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/AFi1xSDK.java
00096	Connect to a URL and set request method	command network	com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java com/revenuecat/purchases/common/HTTPClient.java j2/o.java
00028	Read file from assets directory	file	j2/a.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	l2/p.java
00079	Hide the current app's icon	evasion	z5/m.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/469383317428/namespaces/firebase:fetch?key=AIzaSyB7b154NaqFwNDWI7gt9irTfvzD9PXzImk is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'canShowDeepSleepSoundsPodcast': 'true', 'defaultColorTheme': 'COLOR_TRUE_BLACK', 'interstitialAdMinutesSinceInstallThreshold': '10', 'isCrashingUser': 'false', 'minutesSinceInstallReviewPromptThreshold': '2880', 'minutesSinceInstallRewardedInterstitialAdThreshold': '10080', 'minutesSinceReviewPromptThreshold': '172800', 'numberOfLaunchesReviewPromptThreshold': '2', 'paywallCTAButtonText': 'Redeem Your Free Week', 'premiumSku': 'com.kitefaster.whitenoise.premium_40y_f1w', 'promotions': '{ "youTubePromotions": [], "appPromotions": [], "podcastPromotions": [{ "id": "theSleepyBookshelf", "isShownInSettings": true, "settingsImage": "https://sg-common.nyc3.cdn.digitaloceanspaces.com/remoteConfigAssets/podcast63x75.png", "settingsTitle": "The Sleepy Bookshelf", "settingsDetail": "", "isShownFullScreen": true, "fullScreenDescription": "Fall asleep to classic works of fiction. Try The Sleepy Bookshelf podcast tonight! It\\'s free!", "fullScreenImage": "https://sg-common.nyc3.cdn.digitaloceanspaces.com/remoteConfigAssets/TheSleepyBookshelfAlbumArt.png", "applePodcastsLink": "https://podcasts.apple.com/us/podcast/the-sleepy-bookshelf/id1573623902?mt=2&app=podcast&at=1000lc6i&ct=TheSleepyBookshelf_DSS", "spotifyLink": "https://open.spotify.com/show/0Jj6DoEoG2R5fWdIEbZ0bd", "googlePodcastsLink": "https://podcasts.google.com/feed/aHR0cHM6Ly9hbmNob3IuZm0vcy82MTJkYmQ5MC9wb2RjYXN0L3Jzcw==", "isShownAfterInstallInXDays": 14 }, { "id": "deepSleepSoundsPodcast", "isShownInSettings": true, "settingsImage": "https://sg-common.nyc3.cdn.digitaloceanspaces.com/remoteConfigAssets/podcast63x75.png", "settingsTitle": "Deep Sleep Sounds Podcast", "settingsDetail": "", "isShownFullScreen": true, "fullScreenDescription": "Want more sleep sounds? Listen to the \\\\"Deep Sleep Sounds\\\\" podcast. A free podcast that puts you to sleep.", "fullScreenImage": "https://sg-common.nyc3.cdn.digitaloceanspaces.com/remoteConfigAssets/DeepSleepSoundsPodcastAlbumArt.png", "applePodcastsLink": "https://podcasts.apple.com/us/podcast/deep-sleep-sounds/id1512016028?mt=2&app=podcast&at=1000lc6i&ct=DeepSleepSoundsPodcast_DSS", "spotifyLink": "https://open.spotify.com/show/08OoufgDXbghIZdJsM5dtm", "googlePodcastsLink": "https://podcasts.google.com/feed/aHR0cHM6Ly9hbmNob3IuZm0vcy8xYmNjNmNiMC9wb2RjYXN0L3Jzcw", "isShownAfterInstallInXDays": 28 }, { "id": "getSleepyPodcast", "isShownInSettings": true, "settingsImage": "https://sg-common.nyc3.cdn.digitaloceanspaces.com/remoteConfigAssets/podcast63x75.png", "settingsTitle": "Get Sleepy Podcast", "settingsDetail": "", "isShownFullScreen": true, "fullScreenDescription": "Want sleep inducing stories? Listen to \\\\"Get Sleepy\\\\", the free podcast that puts you to sleep.", "fullScreenImage": "https://sg-common.nyc3.cdn.digitaloceanspaces.com/remoteConfigAssets/GetSleepyAlbumArt.jpg", "applePodcastsLink": "https://podcasts.apple.com/us/podcast/get-sleepy-sleep-meditation-and-stories/id1487513861?mt=2&app=podcast&at=1000lc6i&ct=GetSleepy_DSS", "spotifyLink": "https://open.spotify.com/show/0edOBjruWV6Juxf42WjGxw", "googlePodcastsLink": "https://podcasts.google.com/feed/aHR0cHM6Ly9mZWVkcy5zaW1wbGVjYXN0LmNvbS9JWHhCQnZLeg", "isShownAfterInstallInXDays": 42 }] }', 'requestReviewOnWakeup': 'false', 'reviewRequestConfig': '{ "firstPrompt":{ "minDaysAfterInstall":4, "minLaunches":2, "minKeyEvents":2 }, "secondPrompt":{ "minDaysAfterInstall":10, "minLaunches":4, "minKeyEvents":5 }, "thirdPrompt":{ "minDaysAfterInstall":20, "minLaunches":8, "minKeyEvents":8 }, "additionalPrompts":{ "minDaysAfterInstall":30, "minLaunches":20, "minKeyEvents":20 } }', 'rewardedInterstitialsEnabled': 'false', 'secondsSleepDialogReviewThreshold': '32400', 'sectionHeaderTitleDesign': 'uppercased', 'showAppOpenAd': 'false', 'soundsTableDesign': 'expanded', 'subscriptionScreenVersion': 'menu'}, 'state': 'UPDATE', 'templateVersion': '23'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	4/25	android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	5/44	android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_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
slumberstudios.com	ok	**IP:** 172.67.74.77 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
kitefaster.com	ok	**IP:** 104.21.79.54 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.usenix.org	ok	**IP:** 172.67.159.52 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.googleadservices.com	ok	**IP:** 142.250.188.226 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.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
sinapps.s	ok	No Geolocation information available.
support.google.com	ok	**IP:** 142.250.217.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.rfc-editor.org	ok	**IP:** 104.20.25.136 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.251.40.46 **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:** 142.250.188.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
default.url	ok	No Geolocation information available.
googlemobileadssdk.page.link	ok	**IP:** 142.250.189.1 **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.
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
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.176.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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.
developer.android.com	ok	**IP:** 142.250.217.142 **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.
www.google.com	ok	**IP:** 142.250.72.132 **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.
tools.ietf.org	ok	**IP:** 104.16.44.99 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
sattr.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
bugsnag.com	ok	**IP:** 18.238.96.114 **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.
sars.s	ok	No Geolocation information available.
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
app-measurement.com	ok	**IP:** 142.251.40.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.189.2 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sregister.s	ok	No Geolocation information available.
svalidate.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
deepsleepsounds.nyc3.cdn.digitaloceanspaces.com	ok	**IP:** 104.18.42.227 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
safecurves.cr.yp.to	ok	**IP:** 131.193.32.108 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.880260 **Longitude:** -87.686119 **View:** Google Map
scdn-ssettings.s	ok	No Geolocation information available.
g.co	ok	**IP:** 142.250.72.174 **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.
api-diagnostics.revenuecat.com	ok	**IP:** 34.196.55.80 **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

DOMAIN	STATUS	GEOLOCATION
developer.apple.com	ok	**IP:** 17.253.83.135 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
api-paywalls.revenuecat.com	ok	**IP:** 107.21.207.199 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
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.
sapp.s	ok	No Geolocation information available.
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

DOMAIN	STATUS	GEOLOCATION
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
sviap.s	ok	No Geolocation information available.
google.com	ok	**IP:** 142.250.176.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app.deepsleepsounds.com	ok	**IP:** 172.67.68.49 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
aomedia.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
deepsleepsounds.com	ok	**IP:** 172.67.68.49 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gl	ok	**IP:** 142.250.217.142 **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	ca/p.java
_thumb@3x.jpg _thumb@2x.jpg	q5/h0.java
support@deepsleepsounds.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Bugsnag	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/207
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
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" : "24b937cd21e8474f94b793c0f18777ec"
"google_api_key" : "AIzaSyB7b154NaqFwNDWI7gt9irTfvzD9PXzImk"
"google_crash_reporting_api_key" : "AIzaSyB7b154NaqFwNDWI7gt9irTfvzD9PXzImk"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
9douHjmTTjq3N4YYUdzzHaKyxIqsB5K92p8t26vKQB1HahpVak+32YHan4LmgLPE
V8P78mWO+MxnWR283vMX+BSDXEvrm8XlQCYXMpvUe5w=
3fysZeGzwX+hqd2f4+qtlSho+oF+DeFl9kzKrTFOSWo=
UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMlM=
36864200e0eaf5284d884a0e77d31646
Rx5KxmHu63h8QT7T4cYR2mu7F4LQnYkocG/Azb9HP8ZHyjUHnRxxCuB99BIp3kbl
QcEEfK1PwFv2Eb+NZQ+4kWKAUUVvycYqoBzmAjBexJV/sKEjaFlajeD5MAZYWXy5
JAIugkcNQRXP51pRzjbhWzeihtmzLSCJCmT0+GTbkts=
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
115792089210356248762697446949407573530086143415290314195533631308867097853951
avDZD6/xoSbFYvWCy23XLncB75oD5DxKdrTKFY2O0hY=
Kx8fghNUQq+sA+EfmK6qh0KjuKvw753ECuaCFV8szVM=
7d73d21f1bd82c9e5268b6dcf9fde2cb
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
t+CAjrsoEFEWDgC/oCfdqxFl31lIReQPqb6CaFb+1Y0=
6JHAw9/xzu8LcH4q9f7Udi9sTntehS9dfukXhX8DEHhp54WYBhd6ZhWkqnOAMGmY
fHaUCxrr3fcbpdQPVJw6OSoHeHoizr6wmxmAsnLvDUhuNG2u8ebKX4VPxAoXSx4W
a0784d7a4716f3feb4f64e7f4b39bf04

POSSIBLE SECRETS
115792089210356248762697446949407573529996955224135760342422259061068512044369
ngqbGKXcQCvq0ft27xRzOzNoEVN+ei+Vq2+CNx9QQMc=
u7Ufq5yuXkEXg69T8jpWuOOX55Q9g2DSVI1gtbNUvY8=
bFK3lRg0oaTUwYDrSsMiLa/j4LG9nRlI5KKEyt63x08=
eUrWQVF8FAlcOLX3Auj55rxdEWjF+0P5JAPLCHVKKQw=
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
l4qa5EABhdRHJHltXD4U8dy0wNZl4oyoZ9TbFONnMI4=
vvYcBqgI4aoC3GZZ7n1bdLp71k52s6EJLh0/nA6ME39LmvOZf3TBZ+H4xg1YfQXg
ZdMwT5n8r4APV4u4GhQlb1VCwOIVHkTm7kF7LnArEpyZnsv+C3G3q6fVFgtTcqcc
af60eb711bd85bc1e4d3e0a462e074eea428a8
5kY1EQ+6snGNdZX1BEywItRy0EAwZ4DbRiPucqHAgfZR8kr75HzXIMEIf0cE9z11
0njjbCFUq6vJ1UgnErUI7KEtLgZLN7V9IJ5yZ3QtzXmjMaTjzKInpeDNakYTgh0P
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
KvkOAolI09ZSAixqGUOtipMDBdKXVlslzVnQOpfDZOEJW+xbFKrK173Gu3h1RVkI
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
SKSJAjN3UKeguXyEasCGg04d/yJuUN8XZYgactMp4rfMtHcIJcD0mydl5RKvI49M
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
WGarmwKslNqe3qwfuwVESBFFb2bW57CUuU
tnRfJM39LV6MDlXml8e8fAfi5JhKcsRyFSmagsP97rbE/0XgA5fRVLlLbAYUcu57
FLgp79R6LGLnWDio6G1XBjsjORgKSjLkdakyn5bigQludVyQtVZMhDAlppvakfKf

POSSIBLE SECRETS
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
bae8e37fc83441b16034566b
O+vmm8flr2e7ZrTWUx/T8ClWwcEwLlJlfjM8sMGjZbg=
TvLSh+Eka5RyCXMK4IvAvP4vfksx/KqJwxjzSKu7qQs=
Kq6mcF8LH4HqXGyg5/DR3VvLtDExNTPXoCRIPhkdOGM=
470fa2b4ae81cd56ecbcda9735803434cec591fa
AMztxBQmasdCMrU1nlH2RhtlfSPsjcYFxTHFmKvCDYM=
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
GC4CZUnPsyUcm5NrWw7C8gSktjb/gtBCDrSKBLlqImuOnQy7zHyo6XlIzkH3EMVH
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
gYgEHbtWs2qrOou4Pi9x8/evNQKl7xufkAwk8FBwpKpll2nmAbj5wvKo77J2SETY
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
8E4cUkgIY9w8/0qt+Oeyh9wfu9tQKpeKsR+Ou+hsYewuB4uFdKW1FI4W+bAZwe0B
3071c8717539de5d5353f4c8cd59a032
6jGSPrUM0+2YrTO2vsTOKq3+XL/IfUFs5oxZaSEvsQg=
WfvM4SeNDVyFarUKUVpVTE2MRQkjnaN4GpgwC5lMrmyQkCennlTSSkgCAZvzOVXK
K/sgHSTVeE1LLZ4HP+m5KF6ND+k7W4ID3M3VTul8bAI=
9ObkV+9nuY0gPBNLH25GoxM7YATuF1pi7IORvVFb3+Q=
686479766013060971498190079908139321726943530014330540939446345918554318339765605212255964066145455497729631139148085803712198799971664381257402829111505715 1

POSSIBLE SECRETS
5HcA415u1KU8m2yVlDZBhQQK+0IFNRmmWPxuAq0DnfPzSdJ/uWlnYMD1kKfkH6cZ
NtWyZSC7qBNyKPaXbOjRpNaZGUUAwpDpvYkB4v1ZH9M=
0yxvRSsGg+/BBPRqwe1F54W0T+vv1NRnE+jebtT36Vo=
M2RhhRYJhjrQUa7n9jg23IBcTQvCkUFLA/9ZbQYvHFo=
iz9pI8M74OdFMOjBXhk6CVKK/c29GtinDT3TfbuphLdYOSnoV+Rg8WuW9whaa7rD
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d010104050003820101006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
LYoHKR17UvbUNibqKPKJklawQJNaw1zk7CnhZAC68YBTzC7x4MYQVXp9Sihs98Ok
808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
B3EEABB8EE11C2BE770B684D95219ECB
SHfJbyMgI7MrHewwYoTmYsM7CTkziBSZ0pvzhPCRWcLGoNw6AaEZWLqlKa0dpKuD
lnMUlT0qopStslq/RfZHkyvg0xAUTVuMPsMot4SEaYA=
d7YRusR2mxxBt1bBYjK2gXVvJl/MfqFw2IiZZVeFOFqksQBErGXLOKgf56kYtWpK
g3h/WBQ8k1SqFyNwcX6aXlyabMyZPKS0QgL4qcVfix1XI+70++CdiHkDZKRlUPQw
SkMlFTLt8H3eQLYvgf87g2pXBfp4xPpxL3RMs974XSU=

POSSIBLE SECRETS
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d0101040500308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930313233333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d0030820108028201010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010019d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
SxHy+zpC+eGmQUPW4BYYcldQdVxiSSVnY0gIrWauGKU=

PLAYSTORE INFORMATION

Title: White Noise Deep Sleep Sounds

Score: 4.630268 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.kitefaster.whitenoise

Developer Details: Slumber Studios, 6586831311911659865, None, https://deepsleepsounds.com, support@deepsleepsounds.com,

Release Date: May 21, 2018 **Privacy Policy:** Privacy link

Description:

Check out White Noise Deep Sleep Sounds! Enjoy better sleep at night with the #1 sound machine app for babies with 250+ calming sounds for sleep like HQ white noise, green, brown, pink, and grey as well as rain, ocean, and other nature soundscapes. White Noise and Deep Sleep Sounds help kids and adults sleep better by: - Blocking out unwanted loud distractions with a customizable background noise generator for green, grey, brown, blue, and red options - Forming a calming ambiance that helps you to fall asleep fast and beat insomnia with binaural beats - Helping your baby feel relaxed and soothed with lullabies or calming music - Providing tinnitus therapy, ADHD & anxiety relief by suppressing it with deep brown noise and brain waves With a wide variety of calming music, melodies of rain, binaural beats, brainwaves, and other deep sleep aids, you'll be able to create the perfect ambiance and forget about insomnia. An ultimate aid for a deep rest here. Our white noise machine features a variety of bedtime fan noises and other calming sounds to help you drift off faster if you're a light sleeper or have insomnia. Our noisemaker is fully customizable, allowing you to mix relax melodies and deep sleep sounds to create your nature soundscapes for relaxation. Plus, we have an ASMR section with slime, whispers, and more ASMR sounds guaranteed to give you insomnia relief Our Soundmachine app offers the following soundscape categories: - Industrial - Air Conditioner Sound, Bedtime Fan Noises, Hairdryer sound, Airplane - Nature - Wind, Rain Sounds, Ocean Waves, Thunderstorm Sounds, Fire, Rainforest - Baby - Baby Shushers, Womb, Lullabies - Colored - Brown Noise, Pink Noise, White Noise HQ, Green Noise, as well as Red, Gray, and Blue. Good for tinnitus relief, therapy & masking. - Binaural Beats - 8hz & 4hz frequency, isochronic tones, brain waves generator White Noise and Deep Sleep Aid Fan Sounds help you study and focus by: - Improving your focus and boosting your creativity with green & pink noise - Creating a pleasant and zen-like ambiance for meditation with music Go beyond the standard free white noise machine app with the Premium version, which includes calming sounds of nature. Try the "magic" white noise machine app that has people saying hello to sweet dreams and forget about insomnia! With over 250+ soothing music tracks, "White Noise and Deep Sleep Sounds" is better than an actual sound machine or binaural beats generator. We professionally record all of our calming tracks to add the perfect background noise or ambiance to your bedroom or nursery. Explore our brand new soft sleep music category. The calming music for anxiety and lullabies for babies sections feature relax melodies. The relaxing music & melodies section also includes ambient and atmospheric tones composed exclusively for Deep Sleep Aid Fan Sounds. White Noise Deep Sleep Sounds offers green nature, brown, pink, and grey noises, and bedtime fan sounds to help you calm or relax. Try our sound machine now and sleep better.

SCAN LOGS

Timestamp	Event	Error

2025-08-30 22:35:05	Generating Hashes	OK
2025-08-30 22:35:05	Extracting APK	OK
2025-08-30 22:35:05	Unzipping	OK
2025-08-30 22:35:05	Parsing APK with androguard	OK
2025-08-30 22:35:05	Extracting APK features using aapt/aapt2	OK
2025-08-30 22:35:05	Getting Hardcoded Certificates/Keystores	OK
2025-08-30 22:35:07	Parsing AndroidManifest.xml	OK
2025-08-30 22:35:07	Extracting Manifest Data	OK
2025-08-30 22:35:07	Manifest Analysis Started	OK
2025-08-30 22:35:08	Performing Static Analysis on: Deep Sleep Sounds (com.kitefaster.whitenoise)	OK
2025-08-30 22:35:08	Fetching Details from Play Store: com.kitefaster.whitenoise	OK
2025-08-30 22:35:09	Checking for Malware Permissions	OK
2025-08-30 22:35:09	Fetching icon path	OK
2025-08-30 22:35:09	Library Binary Analysis Started	OK
2025-08-30 22:35:09	Reading Code Signing Certificate	OK

2025-08-30 22:35:10	Running APKiD 2.1.5	OK
2025-08-30 22:35:14	Detecting Trackers	OK
2025-08-30 22:35:16	Decompiling APK to Java with JADX	OK
2025-08-30 22:35:47	Decompiling with JADX failed, attempting on all DEX files	OK
2025-08-30 22:35:47	Decompiling classes2.dex with JADX	OK
2025-08-30 22:35:59	Decompiling classes.dex with JADX	OK
2025-08-30 22:36:14	Decompiling classes2.dex with JADX	OK
2025-08-30 22:36:26	Decompiling classes.dex with JADX	OK
2025-08-30 22:36:40	Converting DEX to Smali	OK
2025-08-30 22:36:40	Code Analysis Started on - java_source	OK
2025-08-30 22:36:46	Android SBOM Analysis Completed	OK
2025-08-30 22:37:00	Android SAST Completed	OK
2025-08-30 22:37:00	Android API Analysis Started	OK
2025-08-30 22:37:11	Android API Analysis Completed	OK
2025-08-30 22:37:12	Android Permission Mapping Started	OK

2025-08-30 22:37:23	Android Permission Mapping Completed	OK
2025-08-30 22:37:24	Android Behaviour Analysis Started	OK
2025-08-30 22:37:38	Android Behaviour Analysis Completed	OK
2025-08-30 22:37:38	Extracting Emails and URLs from Source Code	OK
2025-08-30 22:37:43	Email and URL Extraction Completed	OK
2025-08-30 22:37:43	Extracting String data from APK	OK
2025-08-30 22:37:43	Extracting String data from Code	OK
2025-08-30 22:37:43	Extracting String values and entropies from Code	OK
2025-08-30 22:37:46	Performing Malware check on extracted domains	OK
2025-08-30 22:37:54	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.