MOBSF

ANDROID STATIC ANALYSIS REPORT

NightOwl (3.2.46)

File Name:	com.ectosense.nightowl_500600.apk
Package Name:	com.ectosense.nightowl
Scan Date:	Aug. 29, 2025, 9:58 p.m.
App Security Score:	56/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	12	2	3	1

FILE INFORMATION

File Name: com.ectosense.nightowl_500600.apk
Size: 100.91MB
MD5: a305c33f781552942f2750de773d08f7
SHA1: d6b82dc550aefe7c76c7e8536de89280abbf6e6a
SHA256: 5beefcc0d580f097e7f22445fa44e26f31ad5ea015f3497919dd397de3fc0dff

APP INFORMATION

App Name: NightOwl
Package Name: com.ectosense.nightowl
Main Activity: com.resmed.night.owl.ui.activity.WelcomeActivity
Target SDK: 34
Min SDK: 21
Max SDK:
Android Version Name: 3.2.46
Android Version Code: 500600

APP COMPONENTS

Activities: 8
Services: 9
Receivers: 3
Providers: 6
Exported Activities: 0
Exported Services: 0
Exported Receivers: 1
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: 2018-02-13 11:41:28+00:00
Valid To: 2048-02-13 11:41:28+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xfb886dec60c98ee3f0088115993a6ecce3b6bdb3
Hash Algorithm: sha256
md5: a3c026ca48074d716869ed3183d0a62b
sha1: 1a6ffc85f6b93a81d459cfeb04007e5cadca70d1
sha256: 3bb740e82af4ac503e01a7600841df18467a7454c820f768130557c09f00984c
sha512: ec087de77dc951cff5a5fb98cf532637ae2d8bb1c03a37ccf8ec90cc7b3c59a11261fe3db29306fd1974ce2ca346e17187034e1d6467827c052903c457afe87d
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 296a559b228bc90c6a5fd7817b2a8965eebc7b1a547f79915f483fb1464d4a43
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.HIGH_SAMPLING_RATE_SENSORS	normal	Access higher sampling rate sensor data	Allows an app to access sensor data with a sampling rate greater than 200 Hz.
android.permission.FOREGROUND_SERVICE_CONNECTED_DEVICE	normal	enables foreground services with connected device use.	Allows a regular application to use Service.startForeground with the type "connectedDevice".
android.permission.FOREGROUND_SERVICE_HEALTH	normal	enables foreground services with health-related functionality.	Allows a regular application to use Service.startForeground with the type "health".
android.permission.REQUEST_COMPANION_START_FOREGROUND_SERVICES_FROM_BACKGROUND	normal	allows a companion app to start foreground services from the background.	Allows a companion app to start a foreground service from the background.
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.BLUETOOTH_ADVERTISE	dangerous	required to advertise to nearby Bluetooth devices.	Required to be able to advertise to nearby Bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.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.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.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.BRAND check
Build.DEVICE check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
network operator name check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.resmed.night.owl.ui.activity.WelcomeActivity	Schemes: nightowl://, https://, Hosts: open, nightowl.app.link, nightowl-alternate.app.link,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	secure	Base config is configured to disallow clear text traffic to all domains.

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: **1** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	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.

CODE ANALYSIS

HIGH: **1** | WARNING: **7** | INFO: **1** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/c.java a0/e.java a4/i.java a6/a.java b2/a.java c0/i.java c0/j.java com/airbnb/lottie/LottieAnimationView.java com/blankj/utilcode/util/PermissionUtils.java com/blankj/utilcode/util/ThreadUtils.java com/blankj/utilcode/util/f0.java com/blankj/utilcode/util/h0.java com/blankj/utilcode/util/i.java com/blankj/utilcode/util/p.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/blankj/utilcode/util/q.java com/bumptech/glide/b.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/g.java com/bumptech/glide/load/engine/h.java com/bumptech/glide/load/engine/t.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/c.java com/bumptech/glide/load/resource/bitmap/c0.java com/bumptech/glide/load/resource/bitmap/d.java com/bumptech/glide/load/resource/bitmap/f0.java com/bumptech/glide/load/resource/bitmap/q.java com/bumptech/glide/load/resource/bitmap/r.java com/bumptech/glide/load/resource/bitmap/v.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/manager/d.java com/bumptech/glide/manager/e.java com/bumptech/glide/request/SingleRequest.java com/coolindicator/sdk/CoolIndicator.java com/franmontiel/persistentcookiejar/persistence/SerializableCookie.java com/journeyapps/barcodescanner/CameraPreview.java com/journeyapps/barcodescanner/camera/a.java com/journeyapps/barcodescanner/camera/b.java com/journeyapps/barcodescanner/d.java com/just/agentweb/AgentWebUtils.java com/just/agentweb/AgentWebView.java com/just/agentweb/DefaultChromeClient.java com/just/agentweb/JsCallJava.java com/just/agentweb/JsCallback.java com/just/agentweb/LogUtils.java com/resmed/night/ext/util/a.java com/resmed/night/navigation/FragmentNavigatorHideShow.java com/resmed/night/network/interceptor/logging/LogInterceptor.java com/resmed/night/owl/data/sensor/AbstractRecorder.java com/resmed/night/owl/data/sensor/NightOwlRecorder.java com/resmed/night/owl/service/MyFirebaseMessagingService.java com/resmed/night/owl/ui/activity/WelcomeActivity.java com/resmed/night/owl/ui/fragment/owl/OwlConnectingFragment.java com/resmed/night/owl/ui/fragment/owl/OwlConnectingSensorsFragment.java com/resmed/night/owl/viewmodel/request/OwlUploadFileViewModel.java com/tencent/mmkv/MMKV.java d0/e.java d0/i.java e0/a.java f0/c.java f0/d.java f0/f.java f0/s.java f0/t.java g7/c.java h0/j.java h4/g.java h4/o.java i5/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/branch/referral/BranchJsonConfig.java io/branch/referral/t.java k4/f.java l0/a.java l0/c.java l0/h.java l1/a.java me/jessyan/autosize/AutoSize.java me/jessyan/autosize/AutoSizeConfig.java me/jessyan/autosize/DefaultAutoAdaptStrategy.java me/jessyan/autosize/utils/AutoSizeLog.java me/jessyan/retrofiturlmanager/RetrofitUrlManager.java n0/c.java n0/d.java n0/i.java n1/c.java n4/o.java o0/d.java o1/h.java q6/i.java r/e.java r0/i.java r6/a.java r6/f.java r6/i.java r6/k.java r6/n.java t0/b.java u/a.java v0/a.java v3/q.java w/b.java x/d.java x/e.java y1/i.java z/b.java z/j.java z/l.java z5/e.java z5/g.java
2	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	i5/a.java
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	b8/a.java b8/b.java c8/a.java g3/k0.java
4	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	a4/v.java
5	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	a7/a.java com/just/agentweb/AgentWebUtils.java defpackage/CustomZipUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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/blankj/utilcode/util/q.java com/blankj/utilcode/util/y.java com/just/agentweb/AgentWebUtils.java
7	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/bumptech/glide/load/engine/c.java com/bumptech/glide/load/engine/m.java com/bumptech/glide/load/engine/r.java com/resmed/night/owl/data/model/bean/ActivationCode.java p4/e.java y/c.java
8	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	f2/m0.java f2/t0.java
9	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/journeyapps/barcodescanner/d.java
10	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	h8/e.java y6/a.java
11	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/just/agentweb/AgentWebConfig.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libmmkv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
3	x86_64/libmmkv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
4	x86_64/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	armeabi-v7a/libmmkv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
6	armeabi-v7a/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
7	armeabi/libmmkv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	armeabi/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
9	x86/libmmkv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
10	x86/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	arm64-v8a/libmmkv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
12	arm64-v8a/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
13	x86_64/libmmkv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	x86_64/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
15	armeabi-v7a/libmmkv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
16	armeabi-v7a/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	armeabi/libmmkv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
18	armeabi/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
19	x86/libmmkv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	x86/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/blankj/utilcode/util/PermissionUtils.java com/blankj/utilcode/util/m.java com/blankj/utilcode/util/q.java com/just/agentweb/AgentWebUtils.java com/just/agentweb/DefaultWebClient.java com/resmed/night/owl/app/ext/b.java io/branch/referral/Branch.java io/branch/referral/l.java q7/a.java
00022	Open a file from given absolute path of the file	file	com/blankj/utilcode/util/t.java com/journeyapps/barcodescanner/d.java com/just/agentweb/AgentWebConfig.java com/just/agentweb/AgentWebUtils.java com/resmed/night/owl/data/sensor/AbstractRecorder.java com/resmed/night/owl/viewmodel/request/OwlRecordRequestViewModel.java o4/d.java p/f.java p/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/blankj/utilcode/util/PermissionUtils.java com/blankj/utilcode/util/m.java com/just/agentweb/AgentWebUtils.java com/just/agentweb/DefaultWebClient.java com/resmed/night/owl/app/ext/b.java io/branch/referral/Branch.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	a0/c.java
00091	Retrieve data from broadcast	collection	com/blankj/utilcode/util/MessengerUtils.java com/resmed/night/owl/ui/activity/MainActivity.java io/branch/referral/Branch.java
00013	Read file and put it into a stream	file	com/blankj/utilcode/util/k0.java com/blankj/utilcode/util/x.java com/bumptech/glide/load/a.java defpackage/CustomZipUtils.java f0/f.java n4/w.java o4/d.java okio/k.java p/f.java p/g.java s4/e.java u4/a.java w/b.java
00012	Read data and put it into a buffer stream	file	com/blankj/utilcode/util/k0.java
00065	Get the country code of the SIM card provider	collection	com/resmed/night/owl/app/common/Continent.java
00132	Query The ISO country code	telephony collection	com/resmed/night/owl/app/common/Continent.java v3/n0.java
00004	Get filename and put it to JSON object	file collection	com/resmed/night/owl/app/util/OwlRecordClient.java
00036	Get resource file from res/raw directory	reflection	com/just/agentweb/AgentWebUtils.java com/resmed/night/owl/app/ext/b.java io/branch/referral/Branch.java me/jessyan/autosize/AutoSize.java
00078	Get the network operator name	collection telephony	io/branch/referral/k0.java
00202	Make a phone call	control	com/just/agentweb/DefaultWebClient.java com/resmed/night/owl/app/ext/b.java
00203	Put a phone number into an intent	control	com/just/agentweb/DefaultWebClient.java com/resmed/night/owl/app/ext/b.java
00096	Connect to a URL and set request method	command network	io/branch/referral/o.java p/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	io/branch/referral/o.java p/b.java z/j.java
00162	Create InetSocketAddress object and connecting to it	socket	o8/f.java o8/j.java
00163	Create new Socket and connecting to it	socket	o8/f.java o8/j.java
00014	Read file into a stream and put it into a JSON object	file	o4/d.java u4/a.java
00005	Get absolute path of file and put it to JSON object	file	o4/d.java
00183	Get current camera parameters and change the setting.	camera	com/journeyapps/barcodescanner/camera/b.java
00089	Connect to a URL and receive input stream from the server	command network	io/branch/referral/o.java z/j.java
00109	Connect to a URL and get the response code	network command	io/branch/referral/o.java z/j.java
00054	Install other APKs from file	reflection	com/just/agentweb/AgentWebUtils.java
00192	Get messages in the SMS inbox	sms	com/just/agentweb/AgentWebUtils.java
00191	Get messages in the SMS inbox	sms	com/just/agentweb/AgentWebUtils.java
00003	Put the compressed bitmap data into JSON object	camera	io/branch/referral/network/a.java
00094	Connect to a URL and read data from it	command network	io/branch/referral/o.java r4/a.java
00123	Save the response to JSON after connecting to the remote server	network command	io/branch/referral/o.java
00108	Read the input stream from given URL	network command	io/branch/referral/o.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://nightowl-companion.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/672809265120/namespaces/firebase:fetch?key=AIzaSyD9sLr30SZCmI3nYx8jehpz9roZYyOMaiY is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'detach_sensor_instructions': '[{ "index": 1, "icon": "finger_instructions", "title": "DETACH_SENSOR_1_TITLE", "subtitle": "DETACH_SENSOR_1_SUBTITLE" }, { "index": 2, "icon": "electrode_patch_instructions", "title": "DETACH_SENSOR_2_TITLE", "subtitle": "DETACH_SENSOR_2_SUBTITLE" }, { "index": 3, "icon": "forehead_instructions", "title": "DETACH_SENSOR_3_TITLE", "subtitle": "DETACH_SENSOR_3_SUBTITLE" }]', 'ksyos_centers': '["5bb1d275d1798f50560006a3","5db18ed521d9ca001bc5a24e"]', 'latest_android_app_version': '3.1.0', 'latest_ios_app_version': '4.1.1', 'latest_supported_app_version': '1.0.0', 'pre_rec_instructions': '[{ "index": 1, "icon": "bed_instruction", "title": "PRE_REC_1_TITLE", "subtitle": "PRE_REC_1_SUBTITLE" }, { "index": 2, "icon": "phone_instruction", "title": "PRE_REC_2_TITLE", "subtitle": "PRE_REC_2_SUBTITLE" }, { "index": 3, "icon": "clock_instruction", "title": "PRE_REC_3_TITLE", "subtitle": "PRE_REC_3_SUBTITLE" }, { "index": 4, "icon": "pillow_instruction", "title": "PRE_REC_4_TITLE", "subtitle": "PRE_REC_4_SUBTITLE" }, { "index": 5, "icon": "battery_instruction", "title": "PRE_REC_5_TITLE", "subtitle": "PRE_REC_5_SUBTITLE" }]', 'pre_recording_instructions': '[{"index":1,"icon":"bed_instruction","title":"You can leave your bed","subtitle":"The sensor will reconnect with your phone once you\'re back in range."},{"index":2,"icon":"phone_instruction","title":"Keep the phone close-by","subtitle":"When you're in bed, keep the phone within 2 meters of the sensor."},{"index":3,"icon":"clock_instruction","title":"We need your full night","subtitle":"Don\'t remove the sensor at night as this might cause the test to fail."},{"index":4,"icon":"pillow_instruction","title":"Keep it comfortable","subtitle":"If the adhesive feels too tight, rewrap it more loosely. Take a new adhesive if required."}, {"index":5,"icon":"battery_instruction","title":"Plug in your phone","subtitle":"NightOwl® might drain your battery and we don\'t want to miss out on data."}]', 'should_use_new_uploader': 'true', 'should_use_recording_uploader': 'true', 'special_codes': '{"SABIC":{"survey":{"id":"5ddd15067ec5d00026877fe5","unit":"5cfa6a7f8bf7473d3f006942"}}}', 'state': 'UPDATE', 'templateVersion': '29'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	10/25	android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.SYSTEM_ALERT_WINDOW, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.CAMERA
Other Common Permissions	8/44	android.permission.FOREGROUND_SERVICE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.CHANGE_NETWORK_STATE, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, 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
www.resmed.com.au	ok	**IP:** 199.60.103.30 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.370129 **Longitude:** -71.086304 **View:** Google Map
survey.ectosense.com	ok	**IP:** 18.238.96.49 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **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
nightowl.care	ok	**IP:** 184.27.223.103 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.850029 **Longitude:** -87.650047 **View:** Google Map
nightowl-companion.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
gateway-app.ectosense.com	ok	**IP:** 18.238.96.40 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **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
github.com	ok	**IP:** 140.82.112.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase.google.com	ok	**IP:** 74.125.136.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developer.android.com	ok	**IP:** 64.233.176.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
gateway-prod.ectosense.com	ok	**IP:** 18.155.173.27 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
journeyapps.com	ok	**IP:** 18.238.96.16 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
forms.zohopublic.com	ok	**IP:** 136.143.190.97 **Country:** United States of America **Region:** California **City:** Pleasanton **Latitude:** 37.685314 **Longitude:** -121.894814 **View:** Google Map
cdn.branch.io	ok	**IP:** 18.238.109.81 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
xml.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
survey-us.ectosense.com	ok	**IP:** 18.155.173.123 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api2.branch.io	ok	**IP:** 18.238.109.38 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sisuhealthgroup.com	ok	**IP:** 76.76.21.21 **Country:** United States of America **Region:** California **City:** Walnut **Latitude:** 34.015400 **Longitude:** -117.858223 **View:** Google Map

EMAILS

EMAIL	FILE
privacy@ectosense.com	com/resmed/night/owl/viewmodel/request/OwlConsentFormRequestViewModel.java

TRACKERS

TRACKER	CATEGORIES	URL
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
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
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"com.google.firebase.crashlytics.mapping_file_id" : "e2ad4281418a4cab84813ff2389a5505"
"library_zxingandroidembedded_author" : "JourneyApps"
"google_api_key" : "AIzaSyD9sLr30SZCmI3nYx8jehpz9roZYyOMaiY"
"google_crash_reporting_api_key" : "AIzaSyD9sLr30SZCmI3nYx8jehpz9roZYyOMaiY"
"firebase_database_url" : "https://nightowl-companion.firebaseio.com"

POSSIBLE SECRETS
4D521001-9E6F-4570-880A-67A5FCB14F12
6019373be3f39323ee5fa171
GUssp28gpj4Ehtinf0g7p1U6G2n1e8Ic8tVmHvWa
4D521002-9E6F-4570-880A-67A5FCB14F12
4D521000-9E6F-4570-880A-67A5FCB14F12
e7LIJYU8iz9phpQLKGD0c9GHZClp2bZeaYdmUOM9
470fa2b4ae81cd56ecbcda9735803434cec591fa
txQfVqgAtW2ZYzWnZ2K646LpqHmAGWVf4PoSlc0D
gui20J91TRiVjjd6tnZTJ5pHpa31wQ

PLAYSTORE INFORMATION

Title: NightOwl Companion

Score: 4.716772 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.ectosense.nightowl

Developer Details: ResMed, ResMed, None, https://nightowl.care/patientsupport, NightOwlSupport@resmed.com,

Release Date: Jun 11, 2018 **Privacy Policy:** Privacy link

Description:

This app allows you to interact with the NightOwl sensor that measures signals from your index finger with a small light sensor to check if you have sleep-related breathing disorders. You can set up the test in a few minutes using the in-app instructional videos. Wear the sensor for the prescribed number of nights to complete the test. Disclaimer: This app may provide information from external medical devices. Before making any medical decisions based on this information, read the device instructions carefully and speak with your healthcare provider.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 21:58:25	Generating Hashes	OK
2025-08-29 21:58:25	Extracting APK	OK
2025-08-29 21:58:25	Unzipping	OK

2025-08-29 21:58:25	Parsing APK with androguard	OK
2025-08-29 21:58:26	Extracting APK features using aapt/aapt2	OK
2025-08-29 21:58:26	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 21:58:28	Parsing AndroidManifest.xml	OK
2025-08-29 21:58:28	Extracting Manifest Data	OK
2025-08-29 21:58:28	Manifest Analysis Started	OK
2025-08-29 21:58:28	Reading Network Security config from network_security_config.xml	OK
2025-08-29 21:58:28	Parsing Network Security config	OK
2025-08-29 21:58:28	Performing Static Analysis on: NightOwl (com.ectosense.nightowl)	OK
2025-08-29 21:58:29	Fetching Details from Play Store: com.ectosense.nightowl	OK
2025-08-29 21:58:30	Checking for Malware Permissions	OK
2025-08-29 21:58:30	Fetching icon path	OK
2025-08-29 21:58:30	Library Binary Analysis Started	OK
2025-08-29 21:58:30	Analyzing lib/arm64-v8a/libmmkv.so	OK
2025-08-29 21:58:30	Analyzing lib/arm64-v8a/libc++_shared.so	OK
2025-08-29 21:58:30	Analyzing lib/x86_64/libmmkv.so	OK

2025-08-29 21:58:30	Analyzing lib/x86_64/libc++_shared.so	OK
2025-08-29 21:58:30	Analyzing lib/armeabi-v7a/libmmkv.so	OK
2025-08-29 21:58:30	Analyzing lib/armeabi-v7a/libc++_shared.so	OK
2025-08-29 21:58:30	Analyzing lib/armeabi/libmmkv.so	OK
2025-08-29 21:58:30	Analyzing lib/armeabi/libc++_shared.so	OK
2025-08-29 21:58:30	Analyzing lib/x86/libmmkv.so	OK
2025-08-29 21:58:30	Analyzing lib/x86/libc++_shared.so	OK
2025-08-29 21:58:30	Analyzing apktool_out/lib/arm64-v8a/libmmkv.so	OK
2025-08-29 21:58:30	Analyzing apktool_out/lib/arm64-v8a/libc++_shared.so	OK
2025-08-29 21:58:30	Analyzing apktool_out/lib/x86_64/libmmkv.so	OK
2025-08-29 21:58:30	Analyzing apktool_out/lib/x86_64/libc++_shared.so	OK
2025-08-29 21:58:30	Analyzing apktool_out/lib/armeabi-v7a/libmmkv.so	OK
2025-08-29 21:58:30	Analyzing apktool_out/lib/armeabi-v7a/libc++_shared.so	OK
2025-08-29 21:58:30	Analyzing apktool_out/lib/armeabi/libmmkv.so	OK
2025-08-29 21:58:30	Analyzing apktool_out/lib/armeabi/libc++_shared.so	OK
2025-08-29 21:58:30	Analyzing apktool_out/lib/x86/libmmkv.so	OK

2025-08-29 21:58:30	Analyzing apktool_out/lib/x86/libc++_shared.so	OK
2025-08-29 21:58:30	Reading Code Signing Certificate	OK
2025-08-29 21:58:31	Running APKiD 2.1.5	OK
2025-08-29 21:58:36	Detecting Trackers	OK
2025-08-29 21:58:38	Decompiling APK to Java with JADX	OK
2025-08-29 21:58:50	Converting DEX to Smali	OK
2025-08-29 21:58:50	Code Analysis Started on - java_source	OK
2025-08-29 21:58:52	Android SBOM Analysis Completed	OK
2025-08-29 21:58:58	Android SAST Completed	OK
2025-08-29 21:58:58	Android API Analysis Started	OK
2025-08-29 21:59:03	Android API Analysis Completed	OK
2025-08-29 21:59:03	Android Permission Mapping Started	OK
2025-08-29 21:59:08	Android Permission Mapping Completed	OK
2025-08-29 21:59:08	Android Behaviour Analysis Started	OK
2025-08-29 21:59:14	Android Behaviour Analysis Completed	OK
2025-08-29 21:59:14	Extracting Emails and URLs from Source Code	OK

2025-08-29 21:59:16	Email and URL Extraction Completed	OK
2025-08-29 21:59:16	Extracting String data from APK	OK
2025-08-29 21:59:16	Extracting String data from SO	OK
2025-08-29 21:59:16	Extracting String data from Code	OK
2025-08-29 21:59:16	Extracting String values and entropies from Code	OK
2025-08-29 21:59:19	Performing Malware check on extracted domains	OK
2025-08-29 21:59:24	Saving to Database	OK