MOBSF

ANDROID STATIC ANALYSIS REPORT

Nursa (3.16.2)

File Name:	com.nursa_2000063.apk
Package Name:	com.nursa
Scan Date:	Sept. 1, 2025, 2:37 a.m.

App Security Score: 55/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	12	3	1	1

FILE INFORMATION

File Name: com.nursa_2000063.apk
Size: 38.04MB
MD5: c7794d37fb9c45d0f86a1e6e32914671
SHA1: 39eec8bb70224e350b9bd323c20048005058d3c3
SHA256: c61709432cb9a836a336f06becf97bb8a4252a8e4437c7b35f9af5fd1af87b12

APP INFORMATION

App Name: Nursa
Package Name: com.nursa
Main Activity: com.nursa.MainActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 3.16.2
Android Version Code: 2000063

APP COMPONENTS

Activities: 8
Services: 6
Receivers: 4
Providers: 3
Exported Activities: 2
Exported Services: 0
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
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: 2019-01-07 21:39:03+00:00
Valid To: 2049-01-07 21:39:03+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xda8e0143c5d7d53b168b2ad779d0b68707db0592
Hash Algorithm: sha256
md5: 04315a204063274e009da6d9fe2e6781
sha1: e22b7d971dcf2cb321c8ff81a77a3b4f11bac695

sha256: 463cb09ec93900767ed0e73d5166144109715be2df04437acfa801449da47a82
sha512: 30f92873a3a59c7920a2debfc8d5a9b4f85adbfc08155a887f3ed1f9aaed6da1c3c5b2508d45ccb685c08dc46f4ff346336bcec55f56229a69229f3a4205db2b
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 34db558a1e8d7a1a2ce4e432f237da5e2f072c40afb6bfa11df2b8bd78e69c8c
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	dangerous	allows reading user-selected image or video files from external storage.	Allows an application to read image or video files from external storage that a user has selected via the permission prompt photo picker. Apps can check this permission to verify that a user has decided to use the photo picker, instead of granting access to READ_MEDIA_IMAGES or READ_MEDIA_VIDEO . It does not prevent apps from accessing the standard photo picker manually. This permission should be requested alongside READ_MEDIA_IMAGES and/or READ_MEDIA_VIDEO , depending on which type of media is desired.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.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.
com.nursa.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: yara_issue — DETAILS: yara issue - dex file recognized by apkid but not yara module FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.PRODUCT check SIM operator check network operator name check ro.kernel.qemu check FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)

<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>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></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.TAGS check
network operator name check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.nursa.MainActivity	Schemes: @string/custom_url_scheme://, https://, Hosts: nursa.page.link, nursa.onelink.me, links.nursa.com, Path Prefixes: /CDLD,
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: **0** | INFO: **1**

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

MANIFEST ANALYSIS

HIGH: **0** | WARNING: **6** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	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.
4	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.
5	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
6	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: **4** | INFO: **2** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/manager/RequestManagerRetriever.java com/getcapacitor/AppUUID.java com/getcapacitor/Plugin.java com/hypertrack/sdk/android/types/GetManifestMetadataValueResponse.java com/segment/analytics/AnalyticsContext.java com/segment/analytics/GetDeviceIdTask.java com/segment/analytics/ProjectSettings.java com/segment/analytics/Properties.java com/segment/analytics/Traits.java com/segment/analytics/integrations/AliasPayload.java com/segment/analytics/integrations/BasePayload.java com/segment/analytics/integrations/GroupPayload.java com/segment/analytics/integrations/IdentifyPayload.java com/segment/analytics/integrations/ScreenPayload.java com/segment/analytics/integrations/TrackPayload.java io/capawesome/capacitorjs/plugins/badge/Badge.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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/appsflyer/internal/AFc1qSDK.java com/appsflyer/internal/AFg1jSDK.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/DefaultOnHeaderDecodedListener.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SingletonConnectivityReceiver.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/getcapacitor/Logger.java com/getcapacitor/community/media/photoviewer/RetHandler.java com/hutchind/cordova/plugins/streamingmedia/SimpleAudioStream.java com/hutchind/cordova/plugins/streamingmedia/SimpleVideoStream.java com/segment/analytics/integrations/Logger.java me/leolin/shortcutbadger/ShortcutBadger.java nl/xservices/plugins/accessor/AbstractCalendarAccessor.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/AFa1zSDK.java com/appsflyer/internal/AFc1fSDK.java
4	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/capacitorjs/plugins/clipboard/Clipboard.java
5	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/capacitorjs/plugins/camera/CameraUtils.java com/getcapacitor/FileUtils.java
6	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/capacitorjs/plugins/camera/CameraUtils.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/appsflyer/internal/AFb1iSDK.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/resource/bitmap/ImageReader.java com/getcapacitor/AndroidProtocolHandler.java
00036	Get resource file from res/raw directory	reflection	com/capacitorjs/plugins/browser/Browser.java com/capacitorjs/plugins/pushnotifications/NotificationChannelManager.java com/getcapacitor/AndroidProtocolHandler.java com/getcapacitor/plugin/util/AssetUtil.java com/segment/analytics/internal/Utils.java me/leolin/shortcutbadger/impl/EverythingMeHomeBadger.java me/leolin/shortcutbadger/impl/HuaweiHomeBadger.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/appsflyer/internal/AFc1cSDK.java com/devmantosh/callnumber/CallNumber.java com/hutchind/cordova/plugins/streamingmedia/SimpleAudioStream.java com/hutchind/cordova/plugins/streamingmedia/SimpleVideoStream.java com/segment/analytics/internal/Utils.java de/einfachhans/emailcomposer/EmailComposer.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java
00091	Retrieve data from broadcast	collection	com/capacitorjs/plugins/pushnotifications/PushNotificationsPlugin.java com/hutchind/cordova/plugins/streamingmedia/SimpleAudioStream.java com/hutchind/cordova/plugins/streamingmedia/SimpleVideoStream.java
00024	Write file after Base64 decoding	reflection file	de/einfachhans/emailcomposer/AssetUtil.java
00089	Connect to a URL and receive input stream from the server	command network	com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/getcapacitor/plugin/util/AssetUtil.java com/hutchind/cordova/plugins/streamingmedia/ImageLoadTask.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/getcapacitor/plugin/util/AssetUtil.java com/hutchind/cordova/plugins/streamingmedia/ImageLoadTask.java
00202	Make a phone call	control	com/devmantosh/callnumber/CallNumber.java
00203	Put a phone number into an intent	control	com/devmantosh/callnumber/CallNumber.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/devmantosh/callnumber/CallNumber.java
00189	Get the content of a SMS message	sms	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java nl/xservices/plugins/accessor/AbstractCalendarAccessor.java
00188	Get the address of a SMS message	sms	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java nl/xservices/plugins/accessor/AbstractCalendarAccessor.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	nl/xservices/plugins/accessor/AbstractCalendarAccessor.java
00009	Put data in cursor to JSON object	file	nl/xservices/plugins/accessor/AbstractCalendarAccessor.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java nl/xservices/plugins/accessor/AbstractCalendarAccessor.java

RULE ID	BEHAVIOUR	LABEL	FILES
00010	Read sensitive data(SMS, CALLLOG) and put it into JSON object	sms calllog collection	nl/xservices/plugins/accessor/AbstractCalendarAccessor.java
00191	Get messages in the SMS inbox	sms	com/getcapacitor/FileUtils.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java nl/xservices/plugins/accessor/AbstractCalendarAccessor.java
00200	Query data from the contact list	collection contact	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java nl/xservices/plugins/accessor/AbstractCalendarAccessor.java
00187	Query a URI and check the result	collection sms calllog calendar	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java nl/xservices/plugins/accessor/AbstractCalendarAccessor.java
00201	Query data from the call log	collection calllog	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java nl/xservices/plugins/accessor/AbstractCalendarAccessor.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/AFh1cSDK.java com/segment/analytics/AnalyticsContext.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00109	Connect to a URL and get the response code	network command	com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java com/bumptech/glide/load/data/HttpUrlFetcher.java
00022	Open a file from given absolute path of the file	file	com/getcapacitor/FileUtils.java com/getcapacitor/plugin/util/AssetUtil.java
00072	Write HTTP input stream into a file	command network file	com/getcapacitor/plugin/util/AssetUtil.java
00094	Connect to a URL and read data from it	command network	com/getcapacitor/plugin/util/AssetUtil.java
00108	Read the input stream from given URL	network command	com/getcapacitor/plugin/util/AssetUtil.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1jSDK.java com/getcapacitor/FileUtils.java
00096	Connect to a URL and set request method	command network	com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java
00028	Read file from assets directory	file	com/getcapacitor/FileUtils.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://nursa-prod.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/1054593865883/namespaces/firebase:fetch?key=AIzaSyCbJHgJ8c8m_eQB2ZwzAwkO_aDGWQCd5r0. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/25	android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.CAMERA, android.permission.VIBRATE, android.permission.ACCESS_NETWORK_STATE, android.permission.RECORD_AUDIO, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	8/44	android.permission.ACCESS_BACKGROUND_LOCATION, com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, android.permission.CALL_PHONE, android.permission.READ_CALENDAR, com.google.android.c2dm.permission.RECEIVE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, 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
sconversions.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
nursa-prod.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
sapp.s	ok	No Geolocation information available.
sinapps.s	ok	No Geolocation information available.
api.ionicjs.com	ok	**IP:** 54.148.43.97 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
sattr.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
svalidate.s	ok	No Geolocation information available.
cdn-settings.segment.com	ok	**IP:** 18.238.93.145 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
HyperTrack	Location	https://reports.exodus-privacy.eu.org/trackers/77
Segment	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/62

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"facebook_client_token" : "ac981ea002fd63aaeaf9e353406a8fb1"
"firebase_database_url" : "https://nursa-prod.firebaseio.com"
"google_api_key" : "AIzaSyCbJHgJ8c8m_eQB2ZwzAwkO_aDGWQCd5r0"
"google_crash_reporting_api_key" : "AIzaSyCbJHgJ8c8m_eQB2ZwzAwkO_aDGWQCd5r0"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
686479766013060971498190079908139321726943530014330540939446345918554318339765605212255964066145455497729631139148085803712198799971664381257402829111505715 1
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7

POSSIBLE SECRETS
115792089210356248762697446949407573530086143415290314195533631308867097853951
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

PLAYSTORE INFORMATION

Title: Nursa™

Score: 4.589286 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.nursa

Developer Details: Nursa INC, 8604361767703961311, None, https://nursa.com, hello@nursa.com,

Release Date: Feb 3, 2020 **Privacy Policy:** Privacy link

Description:

Nursa™ provides nurses everywhere a safe place to find available work in real time, and manage their credentials

SCAN LOGS

Timestamp	Event	Error
2025-09-01 02:37:33	Generating Hashes	OK
2025-09-01 02:37:33	Extracting APK	OK
2025-09-01 02:37:33	Unzipping	OK
2025-09-01 02:37:34	Parsing APK with androguard	OK

2025-09-01 02:37:35	Extracting APK features using aapt/aapt2	OK
2025-09-01 02:37:35	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 02:37:37	Parsing AndroidManifest.xml	OK
2025-09-01 02:37:37	Extracting Manifest Data	OK
2025-09-01 02:37:37	Manifest Analysis Started	OK
2025-09-01 02:37:38	Performing Static Analysis on: Nursa (com.nursa)	OK
2025-09-01 02:37:39	Fetching Details from Play Store: com.nursa	OK
2025-09-01 02:37:41	Checking for Malware Permissions	OK
2025-09-01 02:37:41	Fetching icon path	OK
2025-09-01 02:37:41	Library Binary Analysis Started	OK
2025-09-01 02:37:41	Reading Code Signing Certificate	OK
2025-09-01 02:37:41	Running APKiD 2.1.5	OK
2025-09-01 02:37:44	Detecting Trackers	OK
2025-09-01 02:37:46	Decompiling APK to Java with JADX	OK

2025-09-01 03:04:06	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/c7794d37fb9c45d0f86a1e6e32914671/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/c7794d37fb9c45d0f86a1e6e32914671/c7794d37fb9c45d0f86a1e6e32914671.apk'], 999.9999699220061)
2025-09-01 03:04:06	Converting DEX to Smali	OK
2025-09-01 03:04:06	Code Analysis Started on - java_source	OK
2025-09-01 03:04:08	Android SBOM Analysis Completed	OK
2025-09-01 03:04:17	Android SAST Completed	OK
2025-09-01 03:04:17	Android API Analysis Started	OK
2025-09-01 03:04:23	Android API Analysis Completed	OK
2025-09-01 03:04:24	Android Permission Mapping Started	OK
2025-09-01 03:04:19	Android Permission Mapping Completed	OK
2025-09-01 03:04:19	Android Behaviour Analysis Started	OK
2025-09-01 03:04:26	Android Behaviour Analysis Completed	OK
2025-09-01 03:04:26	Extracting Emails and URLs from Source Code	OK
2025-09-01 03:04:27	Email and URL Extraction Completed	OK
2025-09-01 03:04:27	Extracting String data from APK	OK

2025-09-01 03:04:27	Extracting String data from Code	OK
2025-09-01 03:04:27	Extracting String values and entropies from Code	OK
2025-09-01 03:04:29	Performing Malware check on extracted domains	OK
2025-09-01 03:04:34	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.