ANDROID STATIC ANALYSIS REPORT

Transit Now (5.2.0)

File Name:	base.apk
Package Name:	com.opl.transitnow
Scan Date:	Nov. 27, 2025, 6:20 a.m.
App Security Score:	**40/100 (MEDIUM RISK)**
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
4	17	4	0	1

FILE INFORMATION

File Name: base.apk
Size: 24.92MB
MD5: 542683cde5acf64fdf3cf30d8b931250
SHA1: 936f5eba6fad899cfed886d25b76d5569f3027b6
SHA256: d1cdb0d5812393dadf5cd657567c91db0ae8e4084d22467a25ee0d44c22c2a67

APP INFORMATION

App Name: Transit Now
Package Name: com.opl.transitnow
Main Activity: com.opl.transitnow.activity.stops.StopsActivity
Target SDK: 35
Min SDK: 21
Max SDK:
Android Version Name: 5.2.0
Android Version Code: 255200000

APP COMPONENTS

Activities: 15
Services: 20
Receivers: 16
Providers: 5
Exported Activities: 0
Exported Services: 4
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=CA, ST=Ontario, L=Toronto, CN=John Sintal
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2011-06-11 20:54:20+00:00
Valid To: 2044-06-02 20:54:20+00:00
Issuer: C=CA, ST=Ontario, L=Toronto, CN=John Sintal
Serial Number: 0x4df3d5fc
Hash Algorithm: sha1
md5: dfd32afb8a660dd4ca7a8222200bcfe8
sha1: b7cb5d57e94d6e815e4304a74921b15d2da8d8a6
sha256: c43fb6a1107a790c0e67d1b6dbca89411cb32f13bd651458cbb673eb00bf6563
sha512: b8b38a4d82010a8e9d41e20f17cff675c5be5bd4de86015f75a19a7181a45796e5f755eb0aeb21572e8620dee6a6ef836cea46f78eb7b899613ba067ceef386e
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: d2f4d7ab56beaa6b838d38f057a3ad53e5b7c4931802dfee1ef85ecab7918fc1
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
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.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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_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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.FOREGROUND_SERVICE_SPECIAL_USE	normal	enables special-use foreground services.	Allows a regular application to use Service.startForeground with the type "specialUse".
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.HARDWARE check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></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.PRODUCT check
Build.HARDWARE check
Build.TAGS 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>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.opl.transitnow.activity.stops.StopsActivity	Schemes: https://, Hosts: transitnowapp.com, Path Prefixes: /track,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **2** | 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.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

HIGH: **2** | WARNING: **8** | 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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	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.
4	Broadcast Receiver (com.opl.transitnow.widget.TransitNowAppWidgetProvider) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Service (com.opl.transitnow.service.TransitNowPhoneWearableListenerService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Service (com.opl.transitnow.service.predictions.PredictionNotificationService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Service (com.opl.transitnow.service.pushNotifications.PushFirebaseMessagingService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

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

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/opl/transitnow/activity/billing/BillingActivity.java com/opl/transitnow/activity/stopdetails/StopDetailsActivity.java com/opl/transitnow/nextbusdata/api/remote/actransit/ACTransitRemoteAPIImpl.java com/opl/transitnow/nextbusdata/api/remote/bart/BartRemoteAPIImpl.java com/opl/transitnow/nextbusdata/api/remote/mbta/MbtaRemoteAPIImpl.java dagger/internal/Linker.java dagger/internal/ProvidesBinding.java dagger/internal/codegen/GraphAnalysisProcessor.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	butterknife/ButterKnife.java com/opl/transitnow/frankdu/dagger/BaseIntentService.java com/opl/transitnow/location/approximator/GeoCoordinate.java com/opl/transitnow/nextbusdata/NextbusAgencyConfig.java com/opl/transitnow/service/StartJobIntentServiceReceiver.java com/opl/transitnow/util/refresher/Refresher.java com/opl/transitnow/wearcommunication/MessageToNodeSender.java com/sothree/slidinguppanel/SlidingUpPanelLayout.java com/tooltip/Tooltip.java defpackage/JDOMAbout.java io/realm/BaseRealm.java io/realm/DynamicRealm.java io/realm/Realm.java io/realm/RealmCache.java io/realm/RealmObject.java io/realm/RealmResults.java io/realm/internal/FinalizerRunnable.java io/realm/internal/OsRealmConfig.java io/realm/internal/RealmCore.java io/realm/internal/Util.java org/htmlcleaner/CommandLine.java org/htmlcleaner/ConfigFileTagProvider.java org/jdom/JDOMException.java
3	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/opl/transitnow/favourites/FavouriteBackupManager.java com/opl/transitnow/favourites/FavouriteLegacyImporter.java com/opl/transitnow/util/devtools/RealmExtractor.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/opl/transitnow/util/SystemInfo.java
5	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/opl/transitnow/uicommon/promo/ShareAppPromoDialog.java
6	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/opl/transitnow/activity/stopdetails/list/recylerview/adapter/StopDetailsRecylerViewAdapter.java com/opl/transitnow/firebase/ads/banner/AdmobActivityUtil.java com/opl/transitnow/service/datasync/DataSyncAlarmManager.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/librealm-jni.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.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__strchr_chk', '__vsprintf_chk', '__read_chk', '__vsnprintf_chk', '__FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	armeabi-v7a/librealm-jni.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
3	x86/librealm-jni.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
4	x86_64/librealm-jni.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.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__strchr_chk', '__vsprintf_chk', '__read_chk', '__vsnprintf_chk', '__FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/librealm-jni.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.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__strchr_chk', '__vsprintf_chk', '__read_chk', '__vsnprintf_chk', '__FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	armeabi-v7a/librealm-jni.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
7	x86/librealm-jni.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	x86_64/librealm-jni.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.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__strchr_chk', '__vsprintf_chk', '__read_chk', '__vsnprintf_chk', '__FD_SET_chk']	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/getkeepsafe/relinker/ReLinkerInstance.java com/opl/transitnow/util/devtools/RealmExtractor.java io/realm/RealmConfiguration.java io/realm/internal/OsRealmConfig.java io/realm/internal/OsSharedRealm.java io/realm/internal/Util.java org/jdom/input/SAXBuilder.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/opl/transitnow/activity/stops/CustomerServiceUI.java com/opl/transitnow/activity/stops/NavPromoter.java com/opl/transitnow/activity/stops/NavPromoterGeneric.java com/opl/transitnow/activity/subwaymap/SubwayMapActivity.java com/opl/transitnow/activity/subwaystationinfo/SubwayStationInfoActivity.java com/opl/transitnow/navigation/ActivityNavigator.java com/opl/transitnow/service/predictions/ui/PredictionNotificationLauncher.java com/opl/transitnow/uicommon/promo/GenericPromoter.java com/opl/transitnow/util/MapUtil.java com/opl/transitnow/util/NotificationUtil.java com/opl/transitnow/util/SmsSender.java com/opl/transitnow/util/permissions/AlarmPermissionUtil.java com/opl/transitnow/widget/TransitNowAppWidgetProvider.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/opl/transitnow/activity/stops/CustomerServiceUI.java com/opl/transitnow/navigation/ActivityNavigator.java com/opl/transitnow/service/predictions/ui/PredictionNotificationLauncher.java com/opl/transitnow/util/SmsSender.java com/opl/transitnow/util/permissions/AlarmPermissionUtil.java com/opl/transitnow/widget/TransitNowAppWidgetProvider.java
00096	Connect to a URL and set request method	command network	com/goebl/david/Webb.java com/opl/transitnow/nextbusdata/api/NextbusApiManager.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/goebl/david/Webb.java com/opl/transitnow/nextbusdata/api/NextbusApiManager.java com/opl/transitnow/util/devtools/RealmExtractor.java
00014	Read file into a stream and put it into a JSON object	file	com/goebl/david/Webb.java
00013	Read file and put it into a stream	file	com/getkeepsafe/relinker/elf/ElfParser.java com/goebl/david/Webb.java com/opl/transitnow/util/devtools/RealmExtractor.java okio/Okio.java org/htmlcleaner/HtmlCleaner.java org/jdom/adapters/AbstractDOMAdapter.java
00123	Save the response to JSON after connecting to the remote server	network command	com/goebl/david/Webb.java
00089	Connect to a URL and receive input stream from the server	command network	com/goebl/david/Webb.java com/opl/transitnow/util/devtools/RealmExtractor.java
00030	Connect to the remote server through the given URL	network	com/goebl/david/Webb.java com/opl/transitnow/util/devtools/RealmExtractor.java
00162	Create InetSocketAddress object and connecting to it	socket	com/opl/transitnow/util/SystemInfo.java
00163	Create new Socket and connecting to it	socket	com/opl/transitnow/util/SystemInfo.java
00036	Get resource file from res/raw directory	reflection	com/opl/transitnow/navigation/ActivityNavigator.java com/opl/transitnow/util/NotificationUtil.java com/opl/transitnow/widget/TransitNowAppWidgetProvider.java
00056	Modify voice volume	control	com/opl/transitnow/service/predictions/ui/PredictionSoundPlayer.java

RULE ID	BEHAVIOUR	LABEL	FILES
00072	Write HTTP input stream into a file	command network file	com/opl/transitnow/util/devtools/RealmExtractor.java
00094	Connect to a URL and read data from it	command network	com/opl/transitnow/util/devtools/RealmExtractor.java
00108	Read the input stream from given URL	network command	com/opl/transitnow/util/devtools/RealmExtractor.java
00091	Retrieve data from broadcast	collection	com/opl/transitnow/activity/schedules/StaticSchedulesActivity.java com/opl/transitnow/activity/stopdetails/StopDetailsActivity.java com/opl/transitnow/activity/subwaystationinfo/SubwayStationInfoActivity.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://transit-now-static-schedule.firebaseio.com/
App talks to a Firebase database	info	The app talks to Firebase database at https://transit-now-secondary.firebaseio.com/
Open Firebase database	high	The Firebase database at https://transit-now-toronto-legacy.firebaseio.com/.json is exposed to internet without any authentication

TITLE	SEVERITY	DESCRIPTION
Open Firebase database	high	The Firebase database at https://transitnow-830d3.firebaseio.com/.json is exposed to internet without any authentication
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/267649551469/namespaces/firebase:fetch?key=AIzaSyAQg8Zly4cKsdl7LbxJmayreVVHu027TTc is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'ADAPTIVE_BANNER': 'true', 'AD_PADDING_CONFIG': 'sl,0,0,sd,0,0', 'AGENCY_DB_DATES_CREATED': 'ttc=20200622,mbta=20250717,actransit=20250717', 'AGENCY_NEXTBUS_URL_OVERRIDES': '{"ttc":{"primary":{"url":"https://tndt-bthst-1.dedux.org/nbx","apiKey":"GyzNp0Nr@624K","healthCheckUrl":"https://tndt-bthst-1.dedux.org/v1/healthcheck"},"secondary":{"url":"https://tndt2-wnmp.dedux.org/nbx","apiKey":"GyzNp0Nr@624K","healthCheckUrl":"https://tndt2-wnmp.dedux.org/v1/healthcheck"}}}', 'AGENCY_PREPACKAGED_DATA_V2': '{"mbta":{"3":{"20250717":"https://firebasestorage.googleapis.com/v0/b/transitnow-830d3.appspot.com/o/transit-now%2Fagencies-preloaded%2Fnextbus-mbta-20250717-schema3.realm?alt=media&token=a80a8cfc-b882-4cf1-a161-75a2eacaca5b"}},"actransit":{"3":{"20250717":"https://firebasestorage.googleapis.com/v0/b/transitnow-830d3.appspot.com/o/transit-now%2Fagencies-preloaded%2Fnextbus-actransit-20250717-schema3.realm?alt=media&token=32e02685-957d-435e-978d-27ccd55475be"}}}', 'ALARMS_DISABLED': 'false', 'ALWAYS_PERSIST_INERT_DELTAS': 'true', 'ALWAYS_USE_TTC_V2': 'false', 'ANNOUNCEMENT_URL': 'https://announcement-service-001.ai/etfze', 'BACKUP_TTC_PREDICTIONS': 'false', 'BACKUP_TTC_PREDICTIONS_SOURCE': 'TTC_SIMPLE', 'COMPACT_REALM_ENABLED': 'false', 'DATA_SYNC_SERVICE_ALLOWED': 'true', 'DELTA_SYNC_ACTIVITY_COPY_DB': 'true', 'DELTA_SYNC_ACTIVITY_ENABLED': 'false', 'EXTERNAL_API_URL': 'https://bustime.ttc.ca/bustime/api/v3/', 'FORCE_APP_UPDATE_TYPE_MSG': 'SNACKBAR;Update to the latest version for more accurate predictions!', 'FORCE_USE_STOP_TAG_FOR_PREDICTIONS': 'false', 'FULLSCREEN_ADS_ON_ALL_SCREENS_ENABLED': 'true', 'FULLSCREEN_ADS_ON_STOP_DETAILS_ENABLED': 'false', 'INTERNAL_API_URL': 'https://tndt-bthst-1.dedux.org/v1/', 'LATEST_APP_VERSION': '254870000', 'MAX_MISSING_DELTA_DAYS': '3', 'MAX_RETRIES_PREDICTIONS': '1', 'MAX_RETRIES_PREDICTIONS_UNAVAILABLE': '3', 'MAX_RETRIES_VEHICLES': '2', 'MAX_TTC_PREDICTIONS_MULTIREQUEST': '0', 'MULTI_PRED_RES_STRATS': 'ROUTE_DIFF', 'NB_OUT_OF_SERVICE_MSG': 'still initializing', 'NEXTBUS_DARK': 'false', 'NEXTBUS_FORCED_APP_UPDATE_MIN_VERSION': '254780000', 'NEXTBUS_FORCED_APP_UPDATE_REQUIRED': 'true', 'NEXTBUS_ROUTE_DELTA_FETCHER_ENABLED': 'true', 'NEXTBUS_SERVICE_ALERT_AFFECTED_AGENCY': 'ttc', 'NEXTBUS_SERVICE_ALERT_CRITICAL': 'true', 'NEXTBUS_SERVICE_ALERT_ENABLED': 'false', 'NEXTBUS_SERVICE_ALERT_MSG': "<b>IMPORTANT NOTICE:</b> Real-time predictions are temporarily offline due to technical issues with the TTC's GPS system. You can monitor the status updates at <a href='https://x.com/TTChelps'>x.com/TTChelps</a>. Please refer to the posted schedules for the most up-to-date information on bus timings. Thank you for your understanding and patience.", 'NEXTBUS_SERVICE_ALERT_REVISION': '238', 'NEXTBUS_STOP_METADATA_AVAILABLE': 'true', 'NIGHTLY_DATA_SYNC_ENABLED': 'true', 'NUM_DAYS_BETWEEN_INTERSTITIAL': '3', 'NUM_DAYS_BTWN_HEAVY_VALIDATION': '60', 'PREPACKAGED_DATA_AGENCIES': 'mbta,actransit', 'PREPKGED_DATA_URL_actransit': 'https://firebasestorage.googleapis.com/v0/b/transitnow-830d3.appspot.com/o/transit-now%2Fagencies-preloaded%2Fnextbus-actransit-20250717-schema2.realm?alt=media&token=4500644e-86f1-4c48-8846-5460844e491a', 'PREPKGED_DATA_URL_mbta': 'https://firebasestorage.googleapis.com/v0/b/transitnow-830d3.appspot.com/o/transit-now%2Fagencies-preloaded%2Fnextbus-mbta-20250717-schema2.realm?alt=media&token=c217462e-7c47-46ec-ade0-0a9808d2f1c4', 'PREPKGED_DATA_URL_ttc': 'https://firebasestorage.googleapis.com/v0/b/transitnow-830d3.appspot.com/o/transit-now%2Fagencies-preloaded%2Fnextbus-ttc-

TITLE	SEVERITY	DESCRIPTION
		20200622.realm?alt=media&token=abad6a91-42f7-493f-bdef-0ab9b0f0a438', 'PUSH_DELTA_SYNC': 'false', 'PUSH_DELTA_SYNC_AUTO_ENQUEUE': 'false', 'RT_CONFIG_MODE': 'on_nextbus_error_only', 'STOP_DETAILS_AUTO_STATIC_SCHED': 'true', 'STOP_DETAILS_BANNER_AD_POSITION': 'bottom', 'STOP_LIST_BANNER_AD_POSITION': 'bottom', 'TTC_API_MIGRATION_CONFIG': '{"behavior1":{"enabled":false,"effectiveDate":"2025-11-23","message":"We recommend switching to the new TTC data source for improved reliability and faster updates. Your favourites will be preserved."},"behavior2":{"enabled":false,"effectiveDate":"2025-11-27","message":"The legacy TTC API will shut down on Nov 31, 2025. Switch now to avoid service interruption.","confirmMessage":"The legacy API will stop working soon. You may experience service interruptions. Continue with legacy?"},"behavior3":{"enabled":false,"effectiveDate":"2025-12-05","message":"The legacy TTC API has been shut down. Upgrading to the new data source..."}}', 'TTC_API_MIGRATION_SHOW_TOGGLE': 'true', 'TTC_TARGET_SYNC_DATE': '20251116', 'TTC_V2_API_PROVIDER': 'INTERNAL', 'USE_ALT_DB_PROVIDER': 'true', 'VD_ADS': 'false'}, 'state': 'UPDATE', 'templateVersion': '1315'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	10/25	android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.VIBRATE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	5/44	android.permission.ACCESS_NOTIFICATION_POLICY, com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, 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
nextbus.com	ok	**IP:** 45.60.104.2 **Country:** United States of America **Region:** Colorado **City:** Greenwood Village **Latitude:** 39.617210 **Longitude:** -104.950813 **View:** Google Map
www.facebook.com	ok	**IP:** 31.13.80.36 **Country:** Canada **Region:** Ontario **City:** Toronto **Latitude:** 43.700111 **Longitude:** -79.416298 **View:** Google Map
medium.com	ok	**IP:** 162.159.152.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
realm.io	ok	**IP:** 13.225.196.85 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
www.actransit.org	ok	**IP:** 72.3.173.120 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
eepurl.com	ok	**IP:** 23.201.160.160 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
java.sun.com	ok	**IP:** 23.57.90.151 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.mongodb.com	ok	**IP:** 15.197.167.90 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
jdom.org	ok	**IP:** 204.13.10.92 **Country:** United States of America **Region:** Oregon **City:** Corvallis **Latitude:** 44.517742 **Longitude:** -123.298096 **View:** Google Map
ttcrider.ca	ok	**IP:** 185.251.145.145 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
twitter.com	ok	**IP:** 162.159.140.229 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gl	ok	**IP:** 142.250.69.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
jsyntax.medium.com	ok	**IP:** 162.159.153.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
instagram.com	ok	**IP:** 31.13.80.174 **Country:** Canada **Region:** Ontario **City:** Toronto **Latitude:** 43.700111 **Longitude:** -79.416298 **View:** Google Map
www.ttc.ca	ok	**IP:** 20.39.143.75 **Country:** Canada **Region:** Ontario **City:** Toronto **Latitude:** 43.700111 **Longitude:** -79.416298 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ttc.ca	ok	**IP:** 20.39.143.75 **Country:** Canada **Region:** Ontario **City:** Toronto **Latitude:** 43.700111 **Longitude:** -79.416298 **View:** Google Map
dedux.ca	ok	No Geolocation information available.
api-v3.mbta.com	ok	**IP:** 52.3.34.124 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
ntas.ttc.ca	ok	**IP:** 20.39.143.75 **Country:** Canada **Region:** Ontario **City:** Toronto **Latitude:** 43.700111 **Longitude:** -79.416298 **View:** Google Map
retro.umoiq.com	ok	**IP:** 54.148.57.57 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
transit-now-toronto-legacy.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
transitnowapp.com	ok	**IP:** 151.101.1.195 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
transit-now-static-schedule.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **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

DOMAIN	STATUS	GEOLOCATION
cdn.ttc.ca	ok	**IP:** 13.107.246.35 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
api.actransit.org	ok	**IP:** 44.199.160.6 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
transitnow-830d3.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
nickuhlig.github.io	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xmlpull.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
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
www.google.com	ok	**IP:** 142.250.69.36 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
org.jdom.transform.jdomresult	ok	No Geolocation information available.
transit-now-secondary.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

DOMAIN	STATUS	GEOLOCATION
badratart.com	ok	No Geolocation information available.
issuetracker.google.com	ok	**IP:** 142.250.69.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.mbta.com	ok	**IP:** 34.234.233.172 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
x.com	ok	**IP:** 162.159.140.229 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
org.jdom.transform.jdomsource	ok	No Geolocation information available.
assistant.google.com	ok	**IP:** 142.250.69.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 142.250.69.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.bart.gov	ok	**IP:** 104.18.31.20 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

EMAILS

EMAIL	FILE
support@transitnowapp.com	com/opl/transitnow/constants/LogConstants.java

EMAIL	FILE
support@transitnowapp.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://transitnow-830d3.firebaseio.com"
"nextbus_delta_sync_firebase_database_url" : "https://transit-now-toronto-legacy.firebaseio.com"
"alerts_secondary_api_key" : "AIzaSyCuv87UNlnuLwRBGymzVql0zRoN1TCGS54"
"google_maps_key" : "AIzaSyDLoHkDcYqSL6aSN9gEWxhEQJwl89TsF6Q"
"static_schedule_primary_api_key" : "AIzaSyBtlYx45TCKOG3qskpQidQyy-ekxbzqILQ"

POSSIBLE SECRETS
"alerts_primary_api_key" : "AIzaSyDuOvlwWioUApnvmLWgjMjsdlLSUHxRHoQ"
"google_crash_reporting_api_key" : "AIzaSyAQg8Zly4cKsdl7LbxJmayreVVHu027TTc"
"google_api_key" : "AIzaSyAQg8Zly4cKsdl7LbxJmayreVVHu027TTc"
2E7B2E298F92CF97C09AEDB5FD69BBFC
49f946663a8deb7054212b8adda248c6
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
B3EEABB8EE11C2BE770B684D95219ECB
key=hJ6HCnXMxV3fdBpTnsJ3KptPx
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e69613111630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e69613111630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e69613111630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d010104050003820101006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a

POSSIBLE SECRETS
8A2548FEB1DF86E412B87CCD8D6AD209
00A4F3644EF7A9A5FF626EC7203CAB8C
2BB3A43ED96CE2BE411DAE05BC3F80D0
0abd38a3e65145a29a41630dbe432add
58D5813E72A0FA7C87A5D05884CF517A
B4854F0008E4BA74283AD8F3601C66ED
470fa2b4ae81cd56ecbcda9735803434cec591fa
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
65CF76394D666DE514252E3AA4DD6BCC
c103703e120ae8cc73c9248622f3cd1e

POSSIBLE SECRETS
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d0101040500308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930313233333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010019d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
101970759182593122449
1ebd163bba714091a6ac07146ed13e4b
3D4610655EA332B7B3DA9203F1E139DF

PLAYSTORE INFORMATION

Title: Transit Now - Bus Predictions

Score: 4.25 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Maps & Navigation **Play Store URL:** com.opl.transitnow

Developer Details: Transit Now - Bus & Bike, 4784006597731195749, None, http://www.transitnowapp.com, support@transitnowapp.com,

Release Date: Jul 21, 2015 **Privacy Policy:** Privacy link

Description:

Never miss your bus or streetcar with real-time vehicle tracking. All features 100% free. Transit Now... Not Later! Supported cities include Toronto TTC, Boston MBTA, Oakland AC Transit, Laval STL, LA Metro, Jacksonville JTA, and other NextBus cities. Scroll down to see more. Incredibly fast and simple access to real time bus departures. No more swiping, scrolling, tapping multiple screens. Get on with your life! Customize your favourite stops as you wish. Sort and name them with emojis. Offline static schedules in case you lose connection (TTC only) in the subway. Set a timer & multitask as the assistant tells you when to catch the bus or get off your stop. Service alerts keep you informed of unexpected bus delays, detours, subway closures. Share your arrival time with you friends if you're running late or track your friend's status. Home screen widget and Wear OS support so you don't even need to open the app. Bike share user? Use our dedicated app "Cycle Now." Click here https://goo.gl/38Fdc5 Night mode, clean Material Design, offline SMS, TTC operator mode, subway info and so much more. Download now for free and ride the rocket! Is my city supported? - TTC (Toronto, Ontario) - MBTA (Boston, Massachusetts) - AC Transit (Alameda and Contra Costa, Oakland, California, ACT) - STL - Société de transport de Laval (Laval, Quebec) - Los Angeles Metro (LA METRO) - Jacksonville Transportation Authority, JTA, (Jacksonville, Florida) - RTC RIDE, Reno (Nevada) - ART (Asheville Redefines Transit) - Brockton (BAT) - APL, MIT Maryland - Fairfax - CUE (Virginia) - Radford Transit - Chapel Hill Transit - Fort Worth The T, Trinity Metro, FWTA, The T Got feedback? Let's chat about your commute! @TransitNowApp https://instagram.com/transitnowapp https://facebook.com/transitnowapp https://twitter.com/transitnowapp We're on iOS as well! https://goo.gl/TGSWPj Transit Now is an app that has real-time tracking, schedules, accurate predictions, arrival times, bus tracking, streetcar tracking. This TTC tracker shows subway, rail, offline maps, navigation, planning info for the TTC. All features 100% free. Try it out now!

SCAN LOGS

Timestamp	Event	Error
2025-11-27 06:20:21	Generating Hashes	OK
2025-11-27 06:20:21	Extracting APK	OK
2025-11-27 06:20:21	Unzipping	OK
2025-11-27 06:20:22	Parsing APK with androguard	OK
2025-11-27 06:20:22	Extracting APK features using aapt/aapt2	OK

2025-11-27 06:20:22	Getting Hardcoded Certificates/Keystores	OK
2025-11-27 06:20:25	Parsing AndroidManifest.xml	OK
2025-11-27 06:20:25	Extracting Manifest Data	OK
2025-11-27 06:20:25	Manifest Analysis Started	OK
2025-11-27 06:20:26	Performing Static Analysis on: Transit Now (com.opl.transitnow)	OK
2025-11-27 06:20:27	Fetching Details from Play Store: com.opl.transitnow	OK
2025-11-27 06:20:27	Checking for Malware Permissions	OK
2025-11-27 06:20:27	Fetching icon path	OK
2025-11-27 06:20:27	Library Binary Analysis Started	OK
2025-11-27 06:20:27	Analyzing apktool_out/lib/arm64-v8a/librealm-jni.so	OK
2025-11-27 06:20:27	Analyzing apktool_out/lib/armeabi-v7a/librealm-jni.so	OK

2025-11-27 06:20:27	Analyzing apktool_out/lib/x86/librealm-jni.so	OK
2025-11-27 06:20:27	Analyzing apktool_out/lib/x86_64/librealm-jni.so	OK
2025-11-27 06:20:28	Analyzing lib/arm64-v8a/librealm-jni.so	OK
2025-11-27 06:20:28	Analyzing lib/armeabi-v7a/librealm-jni.so	OK
2025-11-27 06:20:28	Analyzing lib/x86/librealm-jni.so	OK
2025-11-27 06:20:28	Analyzing lib/x86_64/librealm-jni.so	OK
2025-11-27 06:20:28	Reading Code Signing Certificate	OK
2025-11-27 06:20:29	Running APKiD 3.0.0	OK
2025-11-27 06:20:33	Detecting Trackers	OK
2025-11-27 06:20:35	Decompiling APK to Java with JADX	OK
2025-11-27 06:20:59	Converting DEX to Smali	OK

2025-11-27 06:20:59	Code Analysis Started on - java_source	OK
2025-11-27 06:21:04	Android SBOM Analysis Completed	OK
2025-11-27 06:21:06	Android SAST Completed	OK
2025-11-27 06:21:06	Android API Analysis Started	OK
2025-11-27 06:21:09	Android API Analysis Completed	OK
2025-11-27 06:21:09	Android Permission Mapping Started	OK
2025-11-27 06:21:13	Android Permission Mapping Completed	OK
2025-11-27 06:21:14	Android Behaviour Analysis Started	OK
2025-11-27 06:21:16	Android Behaviour Analysis Completed	OK
2025-11-27 06:21:16	Extracting Emails and URLs from Source Code	OK
2025-11-27 06:21:18	Email and URL Extraction Completed	OK

2025-11-27 06:21:18	Extracting String data from APK	OK
2025-11-27 06:21:18	Extracting String data from SO	OK
2025-11-27 06:21:18	Extracting String data from Code	OK
2025-11-27 06:21:18	Extracting String values and entropies from Code	OK
2025-11-27 06:22:31	Performing Malware check on extracted domains	OK
2025-11-27 06:22:35	Saving to Database	OK

Report Generated by - MobSF v4.4.3

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.