MOBSF

ANDROID STATIC ANALYSIS REPORT

Ottawa Transit (3.5.9)

File Name:	base.apk
Package Name:	com.anilvasani.ottawatransit
Scan Date:	Nov. 27, 2025, 5:54 a.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	14	3	0	1

FILE INFORMATION

File Name: base.apk
Size: 11.59MB
MD5: 09d2ddc0272e7e9fc0ba3599a1a3b162
SHA1: 97cc09620989d389aedd41ef8fbe9987cc603785
SHA256: f872b8ea8ca292d59a4dc4c219d28c0302599806c5ff6e0d301ab9cbb545c798

APP INFORMATION

App Name: Ottawa Transit
Package Name: com.anilvasani.ottawatransit
Main Activity: com.anilvasani.myttc.old.Activity.MainActivity
Target SDK: 36
Min SDK: 23
Max SDK:
Android Version Name: 3.5.9

Android Version Code: 92

APP COMPONENTS

Activities: 19
Services: 10
Receivers: 12
Providers: 3
Exported Activities: 0
Exported Services: 1
Exported Receivers: 2
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: 2019-11-08 18:01:05+00:00
Valid To: 2049-11-08 18:01:05+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x2eacf9c84a6ad40c28a310e68fe6941f5984fcba
Hash Algorithm: sha256
md5: 743b0069746bf2f81c979d00815e6774
sha1: 940d0ba7851e751a6aa027473a0f331be7ee67f4
sha256: 1ff092c0fd0ca5bcbe9b6f44f73732f2dc77eb703edb05c215c0d9ec917aa310
sha512: e9c3a2b1ff3c22ac2042f0c87a259c3b9ce73c5d8c4c74c15099290806da4920b403bb1fe5a6384dbb7250ed75f9f4016a911c6c0400c53636eae6a424a810a6
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 77b92be00110f64472e7db26cf9e005dea5c7db54435b516769bb03298057afa
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.FOREGROUND_SERVICE_SPECIAL_USE	normal	enables special-use foreground services.	Allows a regular application to use Service.startForeground with the type "specialUse".
android.permission.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.anilvasani.ottawatransit.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check Build.TAGS check SIM operator check FINDINGS: Compiler — DETAILS: r8

FILE	DETAILS
classes2.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Anti-VM Code</td><td>Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible VM check</td></tr><tr><td>Compiler</td><td>r8</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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

TITLE	SEVERITY	DESCRIPTION
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: 4 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23]	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	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	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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	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.
5	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: **6** | INFO: **2** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	com/anilvasani/myttc/old/Database/a.java com/anilvasani/transitprediction/Database/b.java s1/c.java u3/m0.java u3/v0.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	a5/a1.java a5/e.java a5/i0.java b5/u0.java b5/x0.java b5/z0.java b8/m.java e8/d.java ia/f.java k4/p.java l0/v0.java q/d.java q3/a.java t/f.java x5/a.java y4/j.java y4/j0.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	e9/a.java e9/b.java f9/a.java g4/z.java
4	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	k4/g.java
5	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	h1/c.java n1/x.java s7/c.java
6	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	a8/b.java k2/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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	s7/b.java
8	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	u0/a.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	j4/d2.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	a1/a.java b0/a0.java b0/t.java n1/x.java p1/b.java q2/d.java s0/m.java s0/w.java s7/c.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/anilvasani/myttc/old/Activity/PredictionActivity.java com/anilvasani/myttc/old/Util/x.java e3/a.java f4/s.java i4/a.java y4/h.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/anilvasani/myttc/old/Util/x.java f4/s.java i4/a.java y4/h.java
00036	Get resource file from res/raw directory	reflection	com/anilvasani/myttc/old/Util/x.java com/davemorrissey/labs/subscaleview/SubsamplingScaleImageView.java y4/h.java
00034	Query the current data network type	collection network	j4/s2.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	h1/c.java n1/x.java q2/d.java s0/n.java s0/o.java s0/u.java s0/w.java s1/d.java
00109	Connect to a URL and get the response code	network command	c4/d.java k4/u.java q2/h.java t7/c.java
00175	Get notification manager and cancel notifications	notification	com/anilvasani/myttc/old/Background/VehicleAlarmWorker.java
00096	Connect to a URL and set request method	command network	q2/h.java t7/c.java
00089	Connect to a URL and receive input stream from the server	command network	q2/h.java t7/c.java
00153	Send binary data over HTTP	http	q2/h.java
00012	Read data and put it into a buffer stream	file	a1/a.java q2/d.java
00014	Read file into a stream and put it into a JSON object	file	s7/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	m0/y.java
00079	Hide the current app's icon	evasion	l2/b0.java
00112	Get the date of the calendar event	collection calendar	com/anilvasani/myttc/old/Util/a0.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://citytransit-c8830.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/40607642144/namespaces/firebase:fetch?key=AIzaSyAlzjxOTSzeO5F-MqYxcbGqgiRN3dVYkvE is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'CDAvailable': 'false', 'CollapsableAdInterval': '12', 'LoadRoutePath': 'true', 'MapUpdateIntervalDays': '14', 'NBURL': 'https://retro.umoiq.com/service/publicXMLFeed', 'PredictionFullScreenAdInterval': '10', 'Server': 'false', 'ShowCollapsableAd': 'true', 'ShowRemoveAdsMenu': 'true', 'TransitDataUpdateIntervalDays': '7'}, 'state': 'UPDATE', 'templateVersion': '20'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.VIBRATE, android.permission.WAKE_LOCK
Other Common Permissions	3/44	com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_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
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	**IP:** 142.250.137.104 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 140.82.113.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
support.google.com	ok	**IP:** 142.250.137.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.69.98 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
thecitytransit.com	ok	**IP:** 172.64.80.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
goo.gle	ok	**IP:** 67.199.248.13 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
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
play.google.com	ok	**IP:** 142.250.139.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
anilvasani.com	ok	**IP:** 172.64.80.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.anilvasani.com	ok	**IP:** 172.64.80.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
citytransit-c8830.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
retro.umoiq.com	ok	**IP:** 50.112.187.98 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
plus.google.com	ok	**IP:** 142.250.137.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	y4/v.java
support@anilvasani.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
"MAP_API_KEY" : "AIzaSyBswiKY4sUipOEo9MZH0ePojNkIuy1601U"
"com.google.firebase.crashlytics.mapping_file_id" : "d6b355e337334a54a56126d9a80f22dd"
"firebase_database_url" : "https://citytransit-c8830.firebaseio.com"
"google_api_key" : "AIzaSyAlzjxOTSzeO5F-MqYxcbGqgiRN3dVYkvE"
"google_crash_reporting_api_key" : "AIzaSyAlzjxOTSzeO5F-MqYxcbGqgiRN3dVYkvE"
E6K+C1ogZN29OFWU2j1wUPRhMI7Lv3qBcqHzi1vCWW4=
BmyMgDcmCU2Sb3W+7BYwFVF2xyz2fvoB7J9UEh8ejfYjRI4=
7i2iPrjrwVOXQymI9kbzBw+Saen0JiBKsL25H084g9vqkkZvrS3PC/gXCAaliMdd
G3uOiDc+G0afdWyr5AUjFlh12iz8eesF8YVGFxgDk+06TpIz2cE=
PjHrXBXcXoGkJe75zH8RZ0khapXmOV4o2gX+YgkGdus=
oHImj5OTIs8LNvX9EwNQkQ3bSJ9XioOM1m8VTLsnF8I=

POSSIBLE SECRETS
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e69631163014060355040713 0d4d6f756e7461696e20566965773114301206035504 0a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e060355040313 0764726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e69631163014060355040713 0d4d6f756e7461696e20566965773114301206035504 0a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e060355040313 0764726f69643082012080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e69631163014060355040713 0d4d6f756e7461696e20566965773114301206035504 0a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e060355040313 0764726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d01010405000382010100dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
a0784d7a4716f3feb4f64e7f4b39bf04
UDDHIUrqun7cz3t6d4j2iVVfWcHKtBQnSOoDChOFM5Y=
DWCPizo8GliOc3Wu7RYvClF+xyr2cfsd9pI=
gbI2a8ruQFsh7iJbKP5csiDrRqRaAG+o51RWglq6SF+q1HNUXOxpmDRR6GgQlE1Z
jjLuguQ1TtUBIYvLkWHGRHLEQB49t1f8VaYjdD5pX6Q=

POSSIBLE SECRETS

308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d01010405003081943 10b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307 416e64726f69643110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038034313532333336 35365a170d3335303930313233333635365a308194310b3009060355040613025553311330110603550408 130a43616c69666f726e6961316301406035504071307416e64726f69643110300e060355040b1307416e64 726f69643110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d 01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307 d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d01010405000382010100 19d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b

1Gz3ZRhjJNvXJ0g284S9b/dpVAajMMfg8CE3pBcFNFA=

C7gHksN/1NwyNvzCHdeBzJsOxB75cHtIeny2v2KpeXA=

yCCrg1bENlSzqqs7fgrflgqRoB89Hc58RpoZe38mDWknXggRGBdzPAEdsprm/nAh

ygsxUks9qSJOiPMXEo9qlLCVVsFNNRfyc6WjXaB0M8U=

cOth2BAAthu6X8KDmzC58653OwqftcurhEiV9l+3uxMh7KBnOgbdhGM0zSnSPufi

D3uOnzosAliea3W47xM5C0h8xyk=

B3EEABB8EE11C2BE770B684D95219ECB

POSSIBLE SECRETS
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
ExKA4wjDRRYdztAsabUEoV5NOADo4vSkAwQNa4IGw0yLC0NQlDOhDdBTfDT5YHOb
etp1batKULd2kwg+5GPfxliTu8RjfdN0zKvZOjQe8mU=
f5uC0Q5BJBhs1YfPGy7Wx7MnBjWVUX5JNaW+Lz6dfUOfz0sIXH0KubqvlhiUByWt
gyMGe4SoPVIhBgFM+VlZQFWek2IoqCotue6ayBNgVb95WbB68suDu+Zv4jWiM6iG
sl6J6ogR1CQFBNHXqYqYlsoHhQEQ3GzqykotbgjuxxtAslvwVDD28XhO/FGDcWNY
WhU/3eeIEz43+QqYTIKNH8p88w1+Uh4fQMNHsNTU34U=
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
oaC5CLMjwUmi/i48MFPdrATPzdM8HcSPBi81Io4IqyU=
HmeJjis7GlyZf3q/7hAuGENvzSz7eOY=
lJ67yAwBUtoZhasVqN11g6g6opAmTxjVxzUKxhl0fOhTr4nQH4cVWV7NJy0RD49z
D3yRkCwxAFiRaW6y8gM9GkVvxzjvZPEc
Ake3rgkWMjm+UlOd1Tg3PHccqBbIRJQk3bhyKj5k
cV7R50f2/HQumOgCDB4L1ZcSwVOfPPdtbjhx11w36hE=
ykIQv59ak7YBU+e791IU15tGonhZPUUBXST76bDGm7zXSjUSNn9qtHdf61t20THy

POSSIBLE SECRETS
BHmCgCE6CVCTdmuh6BMjEENgxDvkcvoc+YJcERgbmPs6Tg==
BmiKijo8F1WRYmuu6gg1F1hxxDftaPUM/IRQDQU=
BmCSnCwxEUaNcmWq8xYxBlx13Cv7eese+ZpAGw==
P6F0ZRwWAQfQFwxv0Pq3Kr7GsgVJK2iuMjcPK+Aq3kgEIqqz95IgzklzBsNVE1/z
yl2V2fIFd/+gtM2i3wtw7rRydnC7INCVtpRFdnYEC9BkEYS1KI4o6evRDqm9gjRN
BkCyvAwRMTm0TkOZyDYQMHRR/BfGWZQu16Q1Ljk3pdYDZK5S
H16u7wATM3S4Tl6egTYIeX5f+xfdXtsmmA==
HkeprgsbOny5AEiU1TlfNmpVqAjMRcch17g1
bSUQaKDGEujzsstvFAmuaLuv9mtefCQQKWZn9uZj/LI=
kj+4OypsnIcMTfpnmlGzqqY0pqeQ7F3FRQZTzB0M60E=
71irZxeyztMVPxtkZNjCXCWzc9uBzzqfxPgw1LkoaIGD1YWtoRaLj8ZtqyMHro2I
BhNDAdNbKVCXLou3UwS6SQycA6O/T9ZMbr2NWffNFtsRs3WScUuYHsaYRJ0jHvCA
6Tbgi6IQESKZikJOpZcClcVJxza1rhAf3nfasZu/vDcTd3loITpTNbH23xjyLA5L
eyJwcmltYXJ5S2V5SWQiOjMzMTUxOTk4MTksImtleSI6W3sia2V5RGF0YSI6eyJ0eXBlVXJsIjoidHlwZS5nb29nbGVhcGlzLmNvbS9nb29nbGUuY3J5cHRvLnRpbmsuRWNkc2FQdWJsaWNLZXkiLCJ2YWx1ZSI6IkVnWUlBeEFDR0FFYUlRQVNoRGZwOUM5QjcrMU1nMmJQbHJ5WExPOHVScDd6YWZJMldSYURmR1ZqVmlJaEFJNFZzTmVrcCs0bVY0d2toZlhVb3pQZWs5TjgxcUdlK2plNnhjOFpoQkhQIiwia2V5TWF0ZXJpYWxUeXBlIjoiQVNZTU1FVFJJQ19QVUJMSUMifSwic3RhdHVzIjoiRU5BQkxFRCIsImtleUlkIjozMzE1MTk5ODE5LCJvdXRwdXRQcmVmaXhUeXBlIjoiVElOSyJ9XX0=

POSSIBLE SECRETS
1cbd3130fa23b59692c061c594c16cc0
G3uOiDc+G0afdWyr5AUjFlh12iz8eQ==
5ZNtOO3srzHnbl5PLlxEIuHlg0l+6HDun864hT7P5ko=
GWyVkDYrF1qWZnis7BIjFEdjyTLgcPoN/A==
36864200e0eaf5284d884a0e77d31646
JC98YOkW1OV00In88Kxh39aoA4/Lc5LugpNahl16Tw21h78xPzCO3AkqsFSMWF+O
zRITP136LTX4rFLknKK5s+BdzyKXJ24gjaP1ECV594x04Hyj3q+IVU95/J2vSCm1
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
By5K9EmVfikEcCFMOZQd1jxZLLuKkdFWcNBLbmtQ/cGwaIFZzYRhON9QKnCD3h+X
noWWhxc3WlXIb4cqOg7NtD3uZWHj+L+uVXJvY7XilyA=
HmeElzU6FU2YZHWu4BswBl1kyT3iaOEG/JNHGBoLmw==
XCAdtiyR5t8AMQ7u4CMXLD5NJ9dD+Tw+KRPDn9OS+vQ=
GH2AjC4gAlaSf3mg4BswBkh/2iHgef0c8ZdZFwwFmOslRQ==
v7ewhEi0QRfAHjcos6RExS5aIOB6pcbb0aW+P30gIsQ=
CGiPgSorCUyTbWu/8h89FUJv2jv9YuYG54BUEgMB

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
g107GCb4k6+PXON8scRHoxvRnyAK9ZOpFHjKTWKkbXc=
JcrU7fy5RNbMaDqzZNwiOwL0nfU2rS7VBZgzra8NDIE=
VOVDFi9LxFQe2QWzKEnmStNUha/UwjqmQV12jeIMYds=
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
s+erUKEK0AKg0XrZCH85OEIt0v0u2CGPZAaj/S6Q0Yk=
fPyGoeDuTUuDJV03GsNFpCGRO2J3Ui8HA6QvnuqOeQaxvLcgOY5Y2sf90BXpAioC
GH2AjC4gAlaSf3mg4BswBkh/2iHkdv0G55BAEBUQhe0k
z6GzXqyR8kvBYJKVLhMc9mqmsbq6ZkNeWqgTkONnpqg=
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
CL6HTaJ4+bHVCQXLR1XCftwOp39gWYfgPib+AnvHUWA=
2EDSTVCwfkpT+1duJ+umEyNIZ3jEP0NWyK78oeLPLhI=
Ake3rgkWMjm/WV6IwjgYPC5A+hHdWNcn1PY=
6iuDHA2XEqaGCIdpenyLvoYWzHjKpoW5EjYN40bz5Cs=
m1dpreCDNlkoMOYdr+vmzaz+jSmUZiIrETih78jZTqg=

POSSIBLE SECRETS
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
8W5EiIZWvw8ca0gdEf2baMelwD0v1LgWFEv6AqIRDGIzRlZJKgzzVYcusXATxgKN
znAIQ1vWTnsSA3nf0QmMCBs/bj4g6mmUyXonbfu9VUs=
klWIopX/vpRWeyQx7GUjF52wT93EUJwbeMp05ev02yc=
eyJwcmltYXJ5S2V5SWQiOjMwODI3ODA4ODgsImtleSI6W3sia2V5RGF0YSI6eyJ0eXBlVXJsIjoidHlwZS5nb29nbGVhcGlzLmNvbS9nb29nbGUuY3J5cHRvLnRpbmsuRWNkc2FQdWJsaWNLZXkiLCJ2YWx1ZSI6IkVnWUlBeEFDR0FFYUlRQkEyWW5HaWFpc3pEcGtJcWpjalorUTJ2alFUUldQZjhFcTlkZVlhNFpKa3lJaEFCQWFESTd6QWJkQXVpQmlnOWdHSkJ1VTUzSGg5Z0RCa0t2amswS2tabDhjIiwia2V5TWF0ZXJpYWxUeXBlIjoiQVNZTU1FVFJJQ19QVUJMSUMifSwic3RhdHVzIjoiRU5BQkxFRCIsImtleUlkIjozMDgyNzgwODg4LCJvdXRwdXRQcmVmaXhUeXBlIjoiVElOSyJ9XX0=
Zh6cd+aDndZV+YUcVHG1KoZXWtL97j2QmZXbwOqvXvMv7NRw9MmD/Gx8wRyupV8R
hY1jxg+6DUCngCe0vbxb4cMsyHNENce67SGKWd6hzv8=
HmeElzU6FU2YZHWn4AE9Bktoyzv5Y/0H9g==
hTLiiIA7LJpRClVGwbLw56sBtWYdpFA3KN/lVIAoqlyIo4UMQoQK3mH52LWi8hnG
OKoG374XK3cB1cjYFPuO/Bg6vy6AufzuCyu4QCURxkWhJwL4+NqQjs8XziSHB+CQ
470fa2b4ae81cd56ecbcda9735803434cec591fa
0F2tRPtJ+oackwCEaR1ilzSWBDq3birdEdy954kTVJ/3hlaiiP5kh1SmVilvcwVI
BmiNiSotG1yZf2Og7BI4EE9kzSHoZfMd9ZNbCg==
TJcXhplO1c7oeAlzyyjGCjnhXIAfNaFNWGhya9KHb9++zv8J1h9atpUrZL1Yjg6v

POSSIBLE SECRETS
ffEAQyBH71yR4B2obQT/Qgb3Fo0ajWwFYmmZt2nfIS2fjNh6ir76IWAmhSUkzxpD
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
AWaIgTorHkuYYW6y9h4oEVF12izmZQ==
BHmCgCE6CVCTdmuh6BMjClpxyzX2e/sL+YJcERg=
dFQH+5qiD2PRdi0XHMSOoNm+a3fekCOGUzmH+eYRmk9bJvOb468Cs8O4aRQ5LdYP
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
DWCPizoyE02Vb26y6BkqGEJ5zCHmZ/Ea+ZhR
VYNLVwJcUVwKHNYqtTAMU2Cbdf8xQvz3Fr3MGMTI+Feinwv11ysZpnAq/2AMk2I1
CGiNgzoyE02Vb26y6BkqGEJ5zCHmZ/Ea+ZhR
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
GGyThiQzH0OYf2Oj9xYwEEpvxy7sZfUG/A==
GH2AjC4gAlaSf3mg4BswBkh/2iHoZfMd9ZNbCg==
xLMBD0ZYDeFbDZVCzCownSP8NNmORP0EKF5jeEnOGlb2W22XICiCfQYSI28gi51p
DWCPizo8GliOc3Wk7wE9FUd01zH5cuYJ9pI=

POSSIBLE SECRETS
0isRm8IoYsyXMQyBCJPbREn4r5FwCMP2Q3k9zoXRqyk=
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
i1MP+hbN0GtKV+UrtunReVDE3xh08srd5laBoZPswSp8P1i6BkpyGoiKZr6P+aBQ
af60eb711bd85bc1e4d3e0a462e074eea428a8
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
86254750241babac4b8d52996a675549
71OvRH8RKLL5CGPm3dKOf5cGs3Y2jxvT4WismqAQzm1qJBvyLIz7vuBnvO3+wiyt
bae8e37fc83441b16034566b
CGiNgzo2GE+cbGOp/hY4HVx12y0=
a-95ed6082-b8e9-46e8-a73f-ff56f00f5d9d
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
Fl0NzymWHJhyDpr9GrhyVi62KX+d2kj13lp1AwiYQHKKCKe1X2FxmeM5KLeNR5D2
VaL1Wm3LFQTS8VrG634CJrexcardiZdKd3KQwG0TrmE=
GH2AjC4gA1eZZXir7RgrBkN52y3gefMX94ZQDBcKiA==

POSSIBLE SECRETS
jO4sZLvDsqH0XT1pMychedS7fP8lDaqZlRwqYI2S90Y=
kazSW9iygMpHEkKh5zVqXBXYRU+noi3Tzu4hpFfxZG4=
DWCPizoyE02Vb26y7BIoEUF01zDmY+sO94NbGg==
6ZjnfgvB9wgS+Y8hZDivPhgjxRZbCY4q7zFEc6BukViF66w3fH7pDgMpCmaLCsbG
NQ1lo07HyX6R6o9xhF+JysjB/gJoli3QRzxLpFE7RH8=
sazFFsabltlse3qDY43b32ZnLCjQJ0+CJQYLaEeKmSw=
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
f8L7o2HxjA4p9Z1nQw3E5r6T8yU2iCv0B9kM4sD1f7G3hJ5lK2z0X9cW8vQ6b5N3m1Rg8F2o0Lp7A1e9I4u3Y2t0H8x6W5v4Z1n9Q2w7E3r5T8y6U1i0C9vB8k7M4s3D1f2G0h9J5l8K4z7X3cW2v1Q0b9N8m6A5r4F3o2Lp1E0u9I8y7Y6t5H4x3W2v1Z0n9Q8w7E6r5T4y3U2i1C0v9B8k7M6s5D4f3G2h1J0l9K8z7X6cW5v4Q3b2N1m0Rg9F8o7Lp6A5e4I3u2Y1t0H8x7W6v5Z4n3Q2w1E0r9T8y7U6i5C4v3B2k1M0s9D8f7G6h5J4l3K2z1X0cW9v8Q7b6N5m4A3r2F1o0Lp9E8u7I6y5T4h3W2v1Z0n0Q9w8E7r6T5y4U3i2C1v0B9k8M7s6D5f4G3h2J1l0K9z8X7cW6v5Q4b3N2m1R0g9F8o7L6p5A4e3I2u1Y0t9H8x7W6v5Z4n3Q2w1E0r9T8y7U6i5C4v3B2k1M0s9D8f7G6h5J4l3K2z1X0cW9v8Q7b6N5m4A3r2F1o0Lp9E8u7I6y5T4h3W2

PLAYSTORE INFORMATION

Title: Ottawa Transit: OC Transpo Bus

Score: 4.142857 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Maps & Navigation **Play Store URL:** com.anilvasani.ottawatransit

Developer Details: Vasani Technologies Inc., 8896996339991836939, None, https://anilvasani.com, ottawatransit@anilvasani.com,

Release Date: Nov 8, 2019 **Privacy Policy:** Privacy link

Description:

Get real-time bus and O-Train schedule for OC Transpo and STO (Société de transport de l'Outaouais) transit agencies. Incredibly fast and simple access Easy to find

nearby stops on map Plan trip from A to B using Trip Planner around City of Ottawa 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. Offline transit maps available Share bus arrival time with you friends No data? Donn't worry, you can get bus and o-train arrival times via SMS Customize your favorite stops as you wish. Sort and name them with emojis. Ottawa Transit is an app that uses GTFS data for OC Transpo and STO real-time tracking, schedules, accurate predictions, arrival times, bus tracking, train tracking. This Ottawa tracker shows subway, rail, offline maps, navigation, planning info for the OC Transpo Transit agency. All features 100% free. Try it out now! * Foreground service permission required for an alarm function to work.

SCAN LOGS

Timestamp	Event	Error
2025-11-27 05:54:15	Generating Hashes	OK
2025-11-27 05:54:15	Extracting APK	OK
2025-11-27 05:54:15	Unzipping	OK
2025-11-27 05:54:15	Parsing APK with androguard	OK
2025-11-27 05:54:15	Extracting APK features using aapt/aapt2	OK
2025-11-27 05:54:15	Getting Hardcoded Certificates/Keystores	OK
2025-11-27 05:54:17	Parsing AndroidManifest.xml	OK

2025-11-27 05:54:17	Extracting Manifest Data	OK
2025-11-27 05:54:17	Manifest Analysis Started	OK
2025-11-27 05:54:17	Performing Static Analysis on: Ottawa Transit (com.anilvasani.ottawatransit)	OK
2025-11-27 05:54:18	Fetching Details from Play Store: com.anilvasani.ottawatransit	OK
2025-11-27 05:54:19	Checking for Malware Permissions	OK
2025-11-27 05:54:19	Fetching icon path	OK
2025-11-27 05:54:19	Library Binary Analysis Started	OK
2025-11-27 05:54:19	Reading Code Signing Certificate	OK
2025-11-27 05:54:19	Running APKiD 3.0.0	OK
2025-11-27 05:54:22	Detecting Trackers	OK
2025-11-27 05:54:23	Decompiling APK to Java with JADX	OK

2025-11-27 05:54:40	Converting DEX to Smali	OK
2025-11-27 05:54:40	Code Analysis Started on - java_source	OK
2025-11-27 05:54:45	Android SBOM Analysis Completed	OK
2025-11-27 05:54:46	Android SAST Completed	OK
2025-11-27 05:54:46	Android API Analysis Started	OK
2025-11-27 05:54:50	Android API Analysis Completed	OK
2025-11-27 05:54:50	Android Permission Mapping Started	OK
2025-11-27 05:54:53	Android Permission Mapping Completed	OK
2025-11-27 05:54:54	Android Behaviour Analysis Started	OK
2025-11-27 05:54:57	Android Behaviour Analysis Completed	OK
2025-11-27 05:54:57	Extracting Emails and URLs from Source Code	OK

2025-11-27 05:54:58	Email and URL Extraction Completed	OK
2025-11-27 05:54:58	Extracting String data from APK	OK
2025-11-27 05:54:58	Extracting String data from Code	OK
2025-11-27 05:54:58	Extracting String values and entropies from Code	OK
2025-11-27 05:55:50	Performing Malware check on extracted domains	OK
2025-11-27 05:55:52	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.