APP SCORES

Security Score **50/100**

Trackers Detection **6/432**

FILE INFORMATION

File Name io.voiapp.voi_1190_apps.evozi.com.apk

Size 39.14MB

MD5 97458ea9ba0de21dbadfbcb0a04eb8aa

SHA1 73a0e04c1a5908be0168e613f3d2e314ace25243

SHA256 2d80deedf3707f00828283cc2e4fd1940afcf0718eb4471649fca08086084210

APP INFORMATION

App Name Voi

Package Name io.voiapp.voi

Main Activity

Target SDK 30 Min SDK 21 Max SDK

Android Version Name 3.79.0 Android Version Code 1190

PLAYSTORE INFORMATION

Title Voi – e-scooter & e-bike hire

Score 4.75 Installs 5,000,000+ Price 0 Android Version Support Category Travel & Local Play Store URL io.voiapp.voi

Developer Voi Technology Ab, Developer ID Voi+Technology+Ab

Developer Address None

Developer Website https://www.voi.com/

Developer Email admin@voiapp.io

Release Date Aug 30, 2018 Privacy Policy Privacy link

Description

Rent an e-scooter or e-bike with just a tap on your phone, and get anywhere in the city within minutes. Simply download the free Voi app, create an account and get rolling!

A NEW WAY TO MOVE AROUND
Voi provides a new level of mobility to urban dwellers who want to move around freely and conveniently without compromising the environment. So swap the tube, bus or car (and skip the hassle of parking!) for a shared electric scooter or e-bike and zip around the city in style, while leaving no carbon footprint. Rolling along the streets on an e-scooter or e-bike is the perfect way to explore a new city, or simply experience your own hometown from a different perspective.

GET ROLLING IN NO TIME:
1. Get the free Voi app and create an account.
2. Find an e-scooter or e-bike nearby using the in-app map.
3. Unlock the vehicle by scanning the QR code on the handlebar.
4. Set off on the e-scooter or e-bike and get to your destination in no time.

E-SCOOTER OR E-BIKE?
The Voi electric scooter is an excellent choice for when you need to quickly get somewhere within a somewhat shorter distance, while the e-bike is ideal for longer routes.

PRICING AND PASSES
Ride more for less with a monthly subscription, get a day pass or simply pay as you go. Prices vary depending on the city – check the Voi app for the exact prices that apply in your area.

AROUND THE CORNER, ACROSS THE CONTINENT
Soar along the streets of Europe! Voi lets you explore 100+ towns and cities around the continent, by two wheels. Check to see if there’s an e-scooter or e-bike available where you are – go to cities.voi.com/city.

ROAD SAFETY STARTS WITH YOU
Road safety is everyone’s responsibility. The choices you make while riding an electric scooter or e-bike affect not only you, but all your fellow road users, as well. So let’s get it right!

Be sure to know the rules of the road before setting off on an e-scooter or e-bike. Stick to the bike lanes or close to the side curb, and stay off pavements. Never ride under the influence, and always wear a helmet to keep your head safe. Oh, and no twin-riding – one person per e-scooter or e-bike at a time.

FIRST TIME ON AN E-SCOOTER?
If you haven’t used an electric scooter before – activate reduced-speed mode in the app. This caps the max speed of the scooter, allowing you to start off slow while learning to operate the vehicle.

E-SCOOTER AND E-BIKE PARKING – WHAT APPLIES?
Proper parking is a matter of safety and accessibility. Keep yourself informed of your local rules and regulations in regards to e-scooter and e-bike parking – and follow them. Always park the vehicle standing upright, using the kickstand and be sure not to obstruct the path of pedestrians, cyclists or other

vehicles.

LEARN AND EARN
RideSafe Academy provides micro courses that teach you essential knowledge and helpful tips on local electric scooter and e-bike traffic rules and rider safety – all in a fun and engaging way. Boost your road confidence and get rewarded with a free Voi ride! The courses are freely available to all, and in several languages. Go to ridesafe.voi.com.

3 / 23	2 / 13
EXPORTED ACTIVITIES	EXPORTED SERVICES
View All	View All
1 / 5	0 / 4
EXPORTED RECEIVERS	EXPORTED PROVIDERS
View All	View All

SCAN OPTIONS

DECOMPILED CODE

SIGNER CERTIFICATE

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=SE
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-07-05 10:31:55+00:00
Valid To: 2043-06-29 10:31:55+00:00
Issuer: C=SE
Serial Number: 0x64a07ee1
Hash Algorithm: sha256
md5: bbd26e8573e2416aded870b24e6a7231
sha1: cc4e0f4dfff6f32a5f00d9dcb1989b2687c5020e
sha256: 7181b6e79b334c98d2731a8bd6ecd7e750f0a60dab179b22152efa369c758af0
sha512: 40d0d71642731f2878fbd16af3b9f0a0b79462d2426e4e6a6d65a5d10bcecb8bad89f3124bee058ac031ce7be437088d15292a1ed388c3973a4b07618370cf9a
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 7204424466271f3242dfc04404bc5d1b579a618fb26a97d84f1322fc9dce9288
Found 1 unique certificates
```

APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
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_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
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.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.	
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.	
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.	
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.	
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.	
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.	

Showing 1 to 10 of 14 entries

Previous 1 2 Next

ANDROID API

Search:

API	FILES
Android Notifications	
Base64 Decode	
Base64 Encode	
Certificate Handling	
Content Provider	
Crypto	
Dynamic Class and Dexloading	
Execute OS Command	
Get Android Advertising ID	
Get Cell Location	

Showing 1 to 10 of 39 entries

Previous 1 2 3 4 Next

BROWSABLE ACTIVITIES

Search:

ACTIVITY	INTENT
com.braintreepayments.api.BraintreeBrowserSwitchActivity	**Schemes**: io.voiapp.voi.braintree://,
io.voiapp.voi.BlaBlaRideMainActivity	**Schemes**: voiapp://, https://, **Hosts:** open, scooter, payment, free, scan, link.voiapp.io,
io.voiapp.voi.VoiMainActivity	**Schemes**: voiapp://, https://, **Hosts:** open, scooter, payment, free, scan, pass, loyalty, wallet, ride_history, loyalty_instructions, link.voiapp.io,

Showing 1 to 3 of 3 entries

Previous 1 Next

NETWORK SECURITY

HIGH	WARNING	INFO	SECURE
0	0	0	0

Search:

NO	SCOPE	SEVERITY	DESCRIPTION
No data available in table			

Showing 0 to 0 of 0 entries

Previous Next

CERTIFICATE ANALYSIS

HIGH	WARNING	INFO
0	1	1

Search:

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.
Signed Application	info	Application is signed with a code signing certificate

Showing 1 to 2 of 2 entries

Previous 1 Next

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
3	6	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable upatched 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	OPTIONS
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.	
3	App Link assetlinks.json file not found [android:name=io.voiapp.voi.BlaBlaRideMainActivity] [android:host=https://link.voiapp.io]	high	App Link asset verification URL (https://link.voiapp.io/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.	
4	**Activity-Alias** (io.voiapp.voi.BlaBlaRideMainActivity) is not Protected. An intent-filter exists.	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
5	App Link assetlinks.json file not found [android:name=io.voiapp.voi.VoiMainActivity] [android:host=https://link.voiapp.io]	high	App Link asset verification URL (https://link.voiapp.io/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.	
6	**Activity-Alias** (io.voiapp.voi.VoiMainActivity) is not Protected. An intent-filter exists.	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.	
7	**Activity** (com.braintreepayments.api.BraintreeBrowserSwitchActivity) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
8	**Service** (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. **Permission:** com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.	
9	**Broadcast Receiver** (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.	
10	**Service** (com.google.android.play.core.assetpacks.AssetPackExtractionService) 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.	

Showing 1 to 10 of 10 entries

Previous 1 Next

</> CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SUPPRESSED
0	9	2	2	0

Search:

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
1	The App logs information. Sensitive information should never be logged.	info	**CWE:** CWE-532: Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3		
2	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	**OWASP MASVS:** MSTG-NETWORK-4		
3	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		
4	This App may have root detection capabilities.	secure	**OWASP MASVS:** MSTG-RESILIENCE-1		
5	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		
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		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
7	App can write to App Directory. Sensitive Information should be encrypted.	info	**CWE:** CWE-276: Incorrect Default Permissions **OWASP MASVS:** MSTG-STORAGE-14		
8	IP Address disclosure	warning	**CWE:** CWE-200: Information Exposure **OWASP MASVS:** MSTG-CODE-2		
9	This App may request root (Super User) privileges.	warning	**CWE:** CWE-250: Execution with Unnecessary Privileges **OWASP MASVS:** MSTG-RESILIENCE-1	h0/a/a/a/a/u.java	
10	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	c0/i/b/s/q/c.java	

Showing 1 to 10 of 13 entries

Previous 1 2 Next

SHARED LIBRARY BINARY ANALYSIS

Search:

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libbarhopper_v2.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: ['__vsnprintf_chk']	**True** info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/libcardioDecider.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	arm64-v8a/libcardioRecognizer.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	arm64-v8a/libcardioRecognizer_tegra2.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**False** warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	**True** info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/libembrace-native.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
6	arm64-v8a/libmapbox-gl.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	arm64-v8a/libopencv_core.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.	**False** high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries	**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
				unless Dart FFI is used.					

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	arm64-v8a/libopencv_imgproc.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.	**False** high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries	**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
				unless Dart FFI is used.					
9	armeabi/libcardioDecider.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
10	armeabi-v7a/libbarhopper_v2.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.

Showing 1 to 10 of 68 entries

Previous 1 2 3 4 5 6 7 Next

NIAP ANALYSIS v1.3

Search:

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
No data available in table				

Showing 0 to 0 of 0 entries

Previous Next

FILE ANALYSIS

Search:

NO	ISSUE	FILES
1	Certificate/Key files hardcoded inside the app.	assets/ds-amex.pem assets/ds-discover.cer assets/ds-mastercard.crt assets/ds-visa.crt

Showing 1 to 1 of 1 entries

Previous 1 Next

FIREBASE DATABASE ANALYSIS

Search:

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://voiapp-1198e.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/181661184140/namespaces/firebase:fetch?key=AIzaSyC2ndS_adCwVx1Vl-1n_RmyOlRPTJae_k8. This is indicated by the response: The response code is 403

Showing 1 to 2 of 2 entries

Previous 1 Next

MALWARE LOOKUP

VirusTotal Report | Triage Report | MetaDefender Report | Hybrid Analysis Report

APKiD ANALYSIS

Search:

DEX	DETECTIONS
classes.dex	

Search:

FINDINGS	DETAILS
Anti Debug Code	Debug.isDebuggerConnected() check
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check device ID check subscriber ID check ro.kernel.qemu check possible VM check
Compiler	r8

Showing 1 to 3 of 3 entries

Previous 1 Next

DEX	DETECTIONS
classes2.dex	Search:

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check subscriber ID check emulator file check
Compiler	r8 without marker (suspicious)

Showing 1 to 2 of 2 entries

Previous 1 Next

Showing 1 to 2 of 2 entries

Previous 1 Next

BEHAVIOUR ANALYSIS

Search:

RULE ID	BEHAVIOUR	LABEL	FILES
00002	Open the camera and take picture	camera	com/onfido/android/sdk/capture/ui/camera/face/CameraSource.java

RULE ID	BEHAVIOUR	LABEL	FILES
00004	Get filename and put it to JSON object	file collection	h0/a/a/a/a/a0.java h0/a/a/a/a/b0.java
00005	Get absolute path of file and put it to JSON object	file	h0/a/a/a/a/b0.java h0/a/a/a/a/z.java
00007	Use absolute path of directory for the output media file path	file	com/onfido/android/sdk/capture/ui/camera/face/CameraSource.java
00009	Put data in cursor to JSON object	file	h0/a/a/a/a/a0.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	c0/i/a/e/i/e/d5.java
00012	Read data and put it into a buffer stream	file	a0/l/a/a.java com/appboy/support/WebContentUtils.java
00013	Read file and put it into a stream	file	
00014	Read file into a stream and put it into a JSON object	file	c0/i/b/s/q/c.java h0/a/a/a/a/b0.java
00016	Get location info of the device and put it to JSON object	location collection	bo/app/i2.java h0/a/a/a/a/b0.java

Showing 1 to 10 of 74 entries

Previous 1 2 3 4 5 ... 8 Next

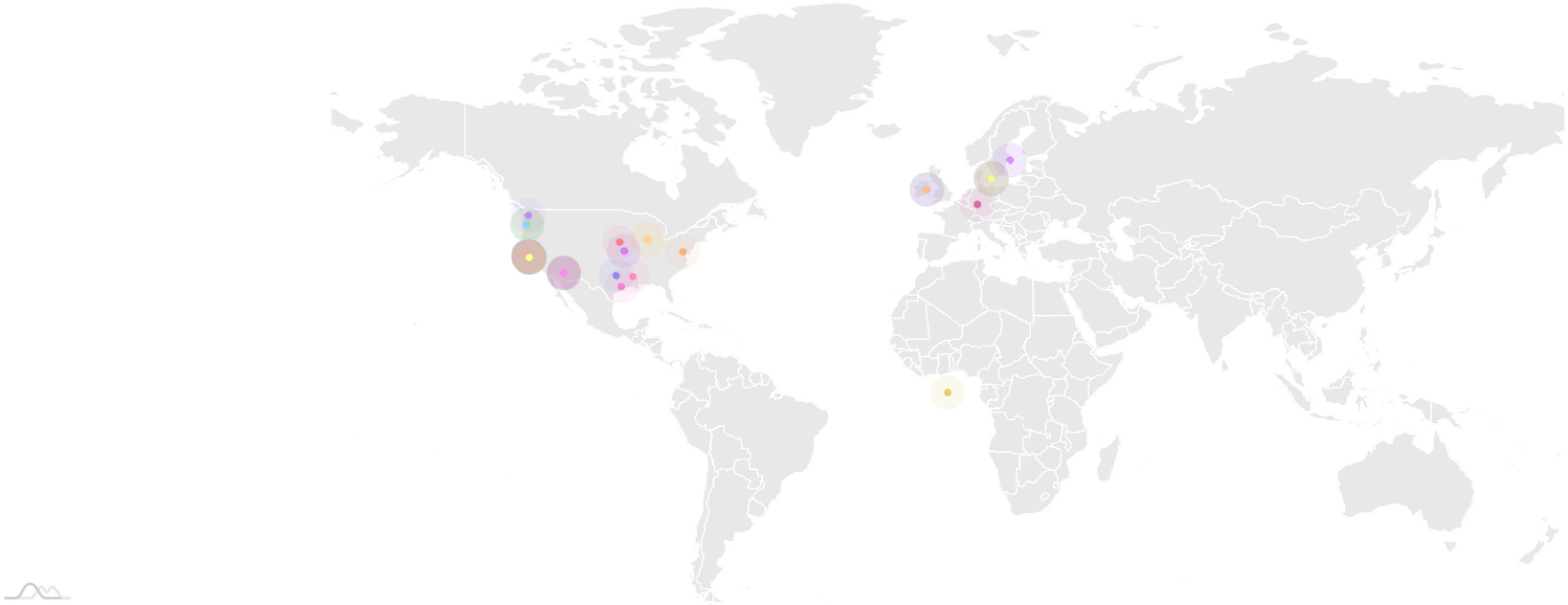
ABUSED PERMISSIONS

Top Malware Permissions	**11**/25	**Other Common Permissions**	**3**/44

android.permission.INTERNET,	android.permission.FOREGROUND_SERVICE,
android.permission.ACCESS_FINE_LOCATION,	com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE,
android.permission.ACCESS_NETWORK_STATE,	com.google.android.c2dm.permission.RECEIVE
android.permission.CAMERA,	
android.permission.RECORD_AUDIO,	
android.permission.VIBRATE, android.permission.WAKE_LOCK,	
android.permission.ACCESS_WIFI_STATE,	
android.permission.WRITE_EXTERNAL_STORAGE,	
android.permission.READ_PHONE_STATE,	
android.permission.READ_EXTERNAL_STORAGE	

Malware Permissions are the top permissions that are widely abused by known malware.
Other Common Permissions are permissions that are commonly abused by known malware.

SERVER LOCATIONS



This app may communicate with the following OFAC sanctioned list of countries.

Search:

DOMAIN	COUNTRY/REGION
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

DOMAIN MALWARE CHECK

Search:

DOMAIN	STATUS	GEOLOCATION
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
accounts.google.com	ok	**IP:** 64.233.163.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
analytics-sdk.onfido.com	ok	**IP:** 63.35.157.227 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
api-m.paypal.com	ok	**IP:** 151.101.87.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api-m.sandbox.paypal.com	ok	**IP:** 151.101.87.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.braintreegateway.com	ok	**IP:** 35.156.167.229 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
api.mapbox.com	ok	**IP:** 13.33.141.96 **Country:** Denmark **Region:** Hovedstaden **City:** Copenhagen **Latitude:** 55.675941 **Longitude:** 12.565530 **View:** Google Map
api.msmaster.qa.paypal.com	ok	No Geolocation information available.
api.onfido.com	ok	**IP:** 13.33.141.6 **Country:** Denmark **Region:** Hovedstaden **City:** Copenhagen **Latitude:** 55.675941 **Longitude:** 12.565530 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.paypal.com	ok	**IP:** 66.211.168.123 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.385639 **Longitude:** -121.885277 **View:** Google Map

Showing 1 to 10 of 78 entries

Previous 1 2 3 4 5 … 8 Next

URLS

Search:

URL	FILE
data:image	c0/e/a/k/u/e.java
file:///	com/appboy/ui/inappmessage/views/AppboyInAppMessageHtmlBaseView.java
file:///android_asset/mavenoid.html	io/voiapp/voi/MainActivity.java
http://%s	io/embrace/android/embracesdk/EmbraceNetworkLoggingService.java
http://10.0.2.2:3000/ https://api.sandbox.braintreegateway.com/ https://api.braintreegateway.com/	c0/d/a/x/c0.java
http://ns.adobe.com/xap/1.0/	a0/l/a/a.java

URL	FILE
http://schemas.android.com/apk/res/android	a0/g/b/b/h.java
http://www.android.com/	c0/f/a/k.java
https://%s/%s/%s	c0/i/b/s/r/c.java
https://accounts.google.com/o/oauth2/revoke?token=	c0/i/a/e/b/a/e/c/f.java

Showing 1 to 10 of 83 entries

Previous 1 2 3 4 5 ... 9 Next

EMAILS

Search:

EMAIL	FILE
android-sdk@onfido.com	com/onfido/android/sdk/capture/OnfidoImpl$handleActivityResult$corruptedResultCallback$1.java
name@example.com your@email.com support@voiapp.io	Android String Resource
support@stripe.com	com/stripe/android/ConnectionFactory.java
support@stripe.com	com/stripe/android/FingerprintRequest.java
support@stripe.com	com/stripe/android/IssuingCardPinService.java
support@stripe.com	com/stripe/android/exception/APIConnectionException.java

EMAIL	FILE
this@mainactivity.lifecycle	io/voiapp/voi/MainActivity$sideMenuLifecycleOwner$1.java
u0013android@android.com u0013android@android.com0	c0/i/a/e/e/a0.java

Showing 1 to 8 of 8 entries

Previous 1 Next

TRACKERS

Search:

TRACKER NAME	CATEGORIES	URL
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
Braze (formerly Appboy)	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/17
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Mapbox		https://reports.exodus-privacy.eu.org/trackers/171

Showing 1 to 6 of 6 entries

Previous 1 Next

🔑 POSSIBLE HARDCODED SECRETS

▶ Show all **498** secrets

A STRINGS

From APK Resource

▶ Show all **10044** strings

From Code

▶ Show all **23417** strings

From Shared Objects

apktool_out/lib/arm64-v8a/libbarhopper_v2.so

▶ Show all **1501** strings

apktool_out/lib/arm64-v8a/libcardioDecider.so

▶ Show all **5** strings

apktool_out/lib/arm64-v8a/libcardioRecognizer.so

▶ Show all **333** strings

apktool_out/lib/arm64-v8a/libcardioRecognizer_tegra2.so

▶ Show all **333** strings

apktool_out/lib/arm64-v8a/libembrace-native.so

▶ Show all **647** strings

apktool_out/lib/arm64-v8a/libmapbox-gl.so

▶ Show all **4429** strings

apktool_out/lib/arm64-v8a/libopencv_core.so

▶ Show all **3036** strings

apktool_out/lib/arm64-v8a/libopencv_imgproc.so

▶ Show all **1213** strings

apktool_out/lib/armeabi/libcardioDecider.so

▶ Show all **22** strings

apktool_out/lib/armeabi-v7a/libbarhopper_v2.so

▶ Show all **1584** strings

apktool_out/lib/armeabi-v7a/libcardioDecider.so

▶ Show all **22** strings

apktool_out/lib/armeabi-v7a/libcardioRecognizer.so

▶ Show all **358** strings

apktool_out/lib/armeabi-v7a/libcardioRecognizer_tegra2.so

▶ Show all **349** strings

apktool_out/lib/armeabi-v7a/libembrace-native.so

▶ Show all **702** strings

apktool_out/lib/armeabi-v7a/libmapbox-gl.so

▶ Show all **4421** strings

apktool_out/lib/armeabi-v7a/libopencv_core.so

▶ Show all **3039** strings

apktool_out/lib/armeabi-v7a/libopencv_imgproc.so

▶ Show all **1220** strings

apktool_out/lib/mips/libcardioDecider.so

▶ Show all **5** strings

apktool_out/lib/x86/libbarhopper_v2.so

▶ Show all **1426** strings

apktool_out/lib/x86/libcardioDecider.so

▼ Showing all **3** strings
/sys/devices/system/cpu/possible
/proc/cpuinfo
/sys/devices/system/cpu/present

apktool_out/lib/x86/libcardioRecognizer.so

▶ Show all **339** strings

apktool_out/lib/x86/libcardioRecognizer_tegra2.so

▶ Show all **12** strings

apktool_out/lib/x86/libembrace-native.so

▶ Show all **668** strings

apktool_out/lib/x86/libmapbox-gl.so

▶ Show all **4387** strings

apktool_out/lib/x86/libopencv_core.so

▶ Show all **3039** strings

apktool_out/lib/x86/libopencv_imgproc.so

▶ Show all **1238** strings

apktool_out/lib/x86_64/libbarhopper_v2.so

▶ Show all **1423** strings

apktool_out/lib/x86_64/libcardioDecider.so

▼ Showing all **3** strings
/sys/devices/system/cpu/possible
/proc/cpuinfo
/sys/devices/system/cpu/present

apktool_out/lib/x86_64/libcardioRecognizer.so

▶ Show all **333** strings

apktool_out/lib/x86_64/libcardioRecognizer_tegra2.so

▶ Show all **333** strings

apktool_out/lib/x86_64/libembrace-native.so

▶ Show all **670** strings

apktool_out/lib/x86_64/libmapbox-gl.so

▶ Show all **4389** strings

apktool_out/lib/x86_64/libopencv_core.so

▶ Show all **3038** strings

apktool_out/lib/x86_64/libopencv_imgproc.so

▶ Show all **1241** strings

lib/arm64-v8a/libbarhopper_v2.so

▶ Show all **1501** strings

lib/arm64-v8a/libcardioDecider.so

▶ Show all **5** strings

lib/arm64-v8a/libcardioRecognizer.so

▶ Show all **333** strings

lib/arm64-v8a/libcardioRecognizer_tegra2.so

▶ Show all **333** strings

lib/arm64-v8a/libembrace-native.so

▶ Show all **647** strings

lib/arm64-v8a/libmapbox-gl.so

▶ Show all **4429** strings

lib/arm64-v8a/libopencv_core.so

▶ Show all **3036** strings

lib/arm64-v8a/libopencv_imgproc.so

▶ Show all **1213** strings

lib/armeabi/libcardioDecider.so

▶ Show all **22** strings

lib/armeabi-v7a/libbarhopper_v2.so

▶ Show all **1584** strings

lib/armeabi-v7a/libcardioDecider.so

▶ Show all **22** strings

lib/armeabi-v7a/libcardioRecognizer.so

▶ Show all **358** strings

lib/armeabi-v7a/libcardioRecognizer_tegra2.so

▶ Show all **349** strings

lib/armeabi-v7a/libembrace-native.so

▶ Show all **702** strings

lib/armeabi-v7a/libmapbox-gl.so

▶ Show all **4421** strings

lib/armeabi-v7a/libopencv_core.so

▶ Show all **3039** strings

lib/armeabi-v7a/libopencv_imgproc.so

▶ Show all **1220** strings

lib/mips/libcardioDecider.so

▶ Show all **5** strings

lib/x86/libbarhopper_v2.so

▶ Show all **1426** strings

lib/x86/libcardioDecider.so

▼ Showing all **3** strings

/sys/devices/system/cpu/possible
/proc/cpuinfo
/sys/devices/system/cpu/present

lib/x86/libcardioRecognizer.so

▶ Show all **339** strings

lib/x86/libcardioRecognizer_tegra2.so

▶ Show all **12** strings

lib/x86/libembrace-native.so

▶ Show all **668** strings

lib/x86/libmapbox-gl.so

▶ Show all **4387** strings

lib/x86/libopencv_core.so

▶ Show all **3039** strings

lib/x86/libopencv_imgproc.so

▶ Show all **1238** strings

lib/x86_64/libbarhopper_v2.so

▶ Show all **1423** strings

lib/x86_64/libcardioDecider.so

▼ Showing all **3** strings
/sys/devices/system/cpu/possible
/proc/cpuinfo
/sys/devices/system/cpu/present

lib/x86_64/libcardioRecognizer.so

▶ Show all **333** strings

lib/x86_64/libcardioRecognizer_tegra2.so

▶ Show all **333** strings

lib/x86_64/libembrace-native.so

▶ Show all **670** strings

lib/x86_64/libmapbox-gl.so

▶ Show all **4389** strings

lib/x86_64/libopencv_core.so

▶ Show all **3038** strings

lib/x86_64/libopencv_imgproc.so

▶ Show all **1241** strings

ACTIVITIES

▼ Showing all **23** activities
io.voiapp.voi.MainActivity
com.braintreepayments.api.BraintreeBrowserSwitchActivity
com.stripe.android.view.AddPaymentMethodActivity
com.stripe.android.view.PaymentMethodsActivity
com.stripe.android.view.PaymentFlowActivity
com.stripe.android.view.PaymentAuthWebViewActivity
com.stripe.android.view.PaymentRelayActivity
com.onfido.android.sdk.capture.ui.OnfidoActivity
com.onfido.android.sdk.capture.ui.camera.CaptureActivity
com.stripe.android.stripe3ds2.views.ChallengeActivity
com.stripe.android.stripe3ds2.views.ChallengeProgressDialogActivity

com.braintreepayments.api.ThreeDSecureActivity
com.appboy.ui.AppboyWebViewActivity
com.appboy.ui.activities.AppboyFeedActivity
com.appboy.ui.activities.AppboyContentCardsActivity
com.appboy.push.AppboyNotificationRoutingActivity
com.google.android.gms.auth.api.signin.internal.SignInHubActivity
io.card.payment.CardIOActivity
io.card.payment.DataEntryActivity
com.google.android.gms.common.api.GoogleApiActivity
com.google.android.play.core.missingsplits.PlayCoreMissingSplitsActivity
com.google.android.play.core.common.PlayCoreDialogWrapperActivity
com.braintreepayments.api.GooglePaymentActivity

SERVICES

▼ Showing all **13** services
io.voiapp.voi.location.TrackRideService
com.appboy.AppboyFirebaseMessagingService
com.braintreepayments.api.internal.AnalyticsIntentService
com.google.firebase.components.ComponentDiscoveryService
com.google.android.gms.auth.api.signin.RevocationBoundService
com.google.firebase.messaging.FirebaseMessagingService
com.google.android.datatransport.runtime.backends.TransportBackendDiscovery
com.mapbox.android.telemetry.crash.CrashReporterJobIntentService
com.google.mlkit.common.internal.MlKitComponentDiscoveryService
com.google.android.gms.measurement.AppMeasurementService
com.google.android.gms.measurement.AppMeasurementJobService
com.google.android.datatransport.runtime.scheduling.jobscheduling.JobInfoSchedulerService
com.google.android.play.core.assetpacks.AssetPackExtractionService

RECEIVERS

▼ Showing all **5** receivers

com.appboy.BrazePushReceiver
com.google.firebase.iid.FirebaseInstanceIdReceiver
com.google.android.gms.measurement.AppMeasurementReceiver
com.google.android.datatransport.runtime.scheduling.jobscheduling.AlarmManagerSchedulerBroadcastReceiver
com.appboy.receivers.AppboyActionReceiver

PROVIDERS

▼ Showing all **4** providers

com.google.firebase.provider.FirebaseInitProvider
com.mapbox.android.telemetry.provider.MapboxTelemetryInitProvider
androidx.lifecycle.ProcessLifecycleOwnerInitializer
com.google.mlkit.common.internal.MlKitInitProvider

LIBRARIES

▼ Showing all **1** libraries

org.apache.http.legacy

SBOM

▼ Showing all **66** Versioned Packages

androidx.activity:activity-ktx@1.2.2
androidx.activity:activity@1.2.2
androidx.annotation:annotation-experimental@1.0.0
androidx.appcompat:appcompat-resources@1.2.0
androidx.appcompat:appcompat@1.2.0
androidx.arch.core:core-runtime@2.1.0
androidx.asynclayoutinflater:asynclayoutinflater@1.0.0
androidx.cardview:cardview@1.0.0
androidx.coordinatorlayout:coordinatorlayout@1.1.0

androidx.core:core-ktx@1.1.0
androidx.core:core@1.3.1
androidx.cursoradapter:cursoradapter@1.0.0
androidx.customview:customview@1.1.0
androidx.databinding:baseAdapters@4.1.1
androidx.databinding:library@4.1.1
androidx.databinding:viewbinding@4.1.1
androidx.documentfile:documentfile@1.0.0
androidx.drawerlayout:drawerlayout@1.1.0
androidx.exifinterface:exifinterface@1.2.0
androidx.fragment:fragment-ktx@1.3.3
androidx.fragment:fragment@1.3.3
androidx.interpolator:interpolator@1.0.0
androidx.legacy:legacy-support-core-ui@1.0.0
androidx.legacy:legacy-support-core-utils@1.0.0
androidx.legacy:legacy-support-v4@1.0.0
androidx.lifecycle:lifecycle-extensions@2.2.0
androidx.lifecycle:lifecycle-livedata-core-ktx@2.3.1
androidx.lifecycle:lifecycle-livedata-core@2.3.1
androidx.lifecycle:lifecycle-livedata@2.2.0
androidx.lifecycle:lifecycle-process@2.2.0
androidx.lifecycle:lifecycle-runtime-ktx@2.3.1
androidx.lifecycle:lifecycle-runtime@2.3.1
androidx.lifecycle:lifecycle-service@2.2.0
androidx.lifecycle:lifecycle-viewmodel-ktx@2.3.1
androidx.lifecycle:lifecycle-viewmodel-savedstate@2.3.1
androidx.lifecycle:lifecycle-viewmodel@2.3.1
androidx.loader:loader@1.0.0
androidx.localbroadcastmanager:localbroadcastmanager@1.0.0
androidx.media:media@1.0.0
androidx.navigation:navigation-common-ktx@2.3.0
androidx.navigation:navigation-common@2.3.0
androidx.navigation:navigation-fragment-ktx@2.3.0
androidx.navigation:navigation-fragment@2.3.0
androidx.navigation:navigation-runtime-ktx@2.3.0
androidx.navigation:navigation-runtime@2.3.0
androidx.navigation:navigation-ui-ktx@2.3.0

androidx.navigation:navigation-ui@2.3.0
androidx.print:print@1.0.0
androidx.recyclerview:recyclerview@1.1.0
androidx.savedstate:savedstate-ktx@1.1.0
androidx.savedstate:savedstate@1.1.0
androidx.slidingpanelayout:slidingpanelayout@1.0.0
androidx.swiperefreshlayout:swiperefreshlayout@1.1.0
androidx.tracing:tracing@1.0.0
androidx.transition:transition@1.3.0
androidx.vectordrawable:vectordrawable-animated@1.1.0
androidx.vectordrawable:vectordrawable@1.1.0
androidx.versionedparcelable:versionedparcelable@1.1.0
androidx.viewpager2:viewpager2@1.0.0
androidx.viewpager:viewpager@1.0.0
androidx.webkit:webkit@1.3.0
com.google.android.material:material@1.2.1
com.google.dagger:dagger-android-support@2.28
com.google.dagger:dagger-android@2.28
com.google.dagger:dagger-lint-aar@2.28
com.google.dagger:dagger@2.28

▶ Show all **263** Packages

FILES

▶ Show all **2097** files