APP SCORES

Security Score **32/100**

Trackers Detection **8/432**

FILE INFORMATION

File Name united-airlines.apk

Size 154.74MB

MD5 e9176955787941ef3c6af69d06acc952

SHA1 a1d164ccc4c8d32561c5d83a937a0a414147902a

SHA256 b71f4c915e0012ed1b009da9b93c5526ff4daaa52c721d1b74bed40fa7a157da

APP INFORMATION

App Name United Airlines

Package Name com.united.mobile.android

Main Activity com.united.mobile.android.ui.splash.SplashActivity

Target SDK 33 Min SDK 28 Max SDK

Android Version Name 4.1.102

Android Version Code 3515

PLAYSTORE INFORMATION

Title United Airlines

Score 4.658679 Installs 10,000,000+ Price 0 Android Version Support Category Travel & Local Play Store URL com.united.mobile.android

Developer United Airlines, Developer ID United+Airlines

Developer Address None

Developer Website https://hub.united.com/united-app-travel-enhancements-2019-2625355292.html

Developer Email ssqa@united.com

Release Date Aug 23, 2011 Privacy Policy Privacy link

Description

Meet the United app

From planning, to booking, to day of travel, we've got you covered.
On our app you can:

- look for flights across our global network and book them easily for yourself, or your friends and family
- check in for your flight and get your boarding pass before you get to the airport
- change seats, or flights, if something better becomes available
- make sure you're prepared for your trip with our Travel-Ready Center
- add your bags, drop them at bag drop shortcut, and track them along your journey
- use our built-in terminal guide to find your gate and navigate the airport with ease
- watch movies, play games, and pay for inflight snacks and drinks while you're in the air
- enroll in MileagePlus or manage your MileagePlus account and use your miles to book award travel in our app
- talk, text or video chat with an agent if you have any questions about your trip
- figure out your next move if your flight is delayed or cancelled

33
ACTIVITIES
View

19
SERVICES
View

17
RECEIVERS
View

11
PROVIDERS
View

Exported Activities
5

Exported Services
2

Exported Receivers
5

Exported Providers
1

SCAN OPTIONS

DECOMPILED CODE

SIGNER CERTIFICATE

```
Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=Illinois, L=Chicago, O=United Airlines, OU=Technology, CN=Michael Natale
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2011-08-22 20:03:34+00:00
Valid To: 2039-01-07 20:03:34+00:00
Issuer: C=US, ST=Illinois, L=Chicago, O=United Airlines, OU=Technology, CN=Michael Natale
Serial Number: 0x4e52b616
Hash Algorithm: sha1
md5: 8dba3d6abdbc5e8537f27529d1976bc8
sha1: 12ec9fbcf3e66e5a12f22cddfbed3ecb3cd415e8
sha256: e833171fd602255f030ed251c64a9989c7eabc4ebe1c3d7b097ae0f9aea8f946
sha512:
1d50bd97ac1a35963ad32bfa2a4092b5a80e7246da5fee3fcd49276557f0e2560fb1483d93e56e6914158fb39b4e14a0f7e7e5e303eda22a6d39
92d169b5ec92
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 53585038eef3d66ed45bda2c04ed2a0a19ed6822f016da4d278e53e0b06861d6
Found 1 unique certificates
```

APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
aero.panasonic.inflight.permission.ACCESS_IFESERVICE	unknown	Unknown permission	Unknown permission from android reference	
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	CODE MAPPINGS
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.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
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.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.	
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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.	
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.	

Showing 1 to 10 of 42 entries

Previous 1 2 3 4 5 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 Installed Applications	

Showing 1 to 10 of 38 entries

Previous 1 2 3 4 Next

BROWSABLE ACTIVITIES

Search:

ACTIVITY	INTENT
com.united.mobile.android.ui.main.MainActivity	**Schemes**: http://, https://, ualentertainment://, ualpartnerprovisionreturn://, ualpartnerprovisioncancel://, ualpaypalreturn://, ualpaypalcancel://, ualmasterpassreturn://, ualprepaidbagsreturn://, uaportalpacstream://, ualmobile://, **Hosts:** www.united.com, united.com, news.united.com, www.unitedwifi.com, openapp, homescreen, mytrips, flights, click.enews.united.com, **Mime Types:** application/pdf, **Paths:** /portal/vod/playmovie, /portal/l/appdetection, /, **Path Prefixes:** /ual/en/us/navigation/airportnav/nav, /ual/en/us/navigation/airportNAV/nav, /ual/en/US/navigation/airportnav/nav, /ual/en/US/navigation/airportNAV/nav, /en/us/fly/travel/airport/terminal-guide/download-app.html, /offers/myoffers, /en/us/flightstatus/details, /ual/en/us/Booking/SearchInjection/VendorQueryPinDown, /ual/en/jp/Booking/SearchInjection/VendorQueryPinDown, /Booking/SearchInjection/VendorQueryPinDown, /en/us/preordermeals/flightinformation, /en/us/preordermeals/deeplink/marketing, /en/us/digital-wallet/checkout, /en/us/checkin, /travel/checkin/quickstart, /en/us/account, /en/us/fly/travel/baggagetracking, /en/us/pbs, /en/us/baggage/issues-with-your-checked-bags, /en-us/flights, /en/us/manageres/mytrips, /s/us, /en/us/fly/travel/mobile-tools/united-trip-planner, /pub/acc, /en/US/manageres/tripdetails, /en/us/manageRes/tripDetails, /en/us/manageres/tripdetails, /en/us/myunited/verify/phone, /en/us/myunited/verify/email,

ACTIVITY	INTENT
	/en/us/fly/print/bagtag, **Path Patterns:** .*,
com.united.mobile.android.ui.main.TravelReadyCenterAlias	**Schemes**: https://, **Hosts:** www.united.com, united.com, **Path Prefixes:** /en/us/travelreadycenter, /travelreadycenter,

Showing 1 to 2 of 2 entries

Previous 1 Next

NETWORK SECURITY

HIGH	WARNING	INFO	SECURE
1	0	0	1

Search:

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

NO	SCOPE	SEVERITY	DESCRIPTION
2	127.0.0.1 172.27.4.91 192.168.1.1 localhost airpana.com gogoinflight.com inflightinternet.com ideanovatech.com inflightpanasonic.aero ufs.ltv jcb-card.jp	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

Showing 1 to 2 of 2 entries

Previous 1 Next

CERTIFICATE ANALYSIS

HIGH	WARNING	INFO
1	0	1

Search:

TITLE	SEVERITY	DESCRIPTION
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.
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
4	14	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application c an older version c multiple vulnerab Android version = receive reasonabl

NO	ISSUE	SEVERITY	DESCRIPTION
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Secu feature lets apps c network security s declarative config modifying app co can be configurec domains and for a
3	**Activity** (com.united.mobile.android.ui.NfcActivity) is not Protected. [android:exported=true]	warning	An Activity is foun other apps on the leaving it accessib application on the

NO	ISSUE	SEVERITY	DESCRIPTION
4	App Link assetlinks.json file not found [android:name=com.united.mobile.android.ui.main.MainActivity] [android:host=https://www.united.com]	high	App Link asset ve (https://www.unit known/assetlinks configured incorr None). App Links redirect from a we mobile app. If this incorrectly config Link host/domain can hijack such U to phishing attack data in the URI, su tokens, magic link tokens and more. App Link domain assetlinks.json fil verification via [android:autoVeri Activity intent-filt

NO	ISSUE	SEVERITY	DESCRIPTION
5	App Link assetlinks.json file not found [android:name=com.united.mobile.android.ui.main.MainActivity] [android:host=https://united.com]	high	App Link asset ve (https://united.co known/assetlinks configured incorr 302). App Links al redirect from a we mobile app. If this incorrectly config Link host/domain can hijack such U to phishing attack data in the URI, su tokens, magic link tokens and more. App Link domain assetlinks.json file verification via [android:autoVeri Activity intent-filt

NO	ISSUE	SEVERITY	DESCRIPTION
6	App Link assetlinks.json file not found [android:name=com.united.mobile.android.ui.main.MainActivity] [android:host=https://www.unitedwifi.com]	high	App Link asset ve (https://www.unit known/assetlinks configured incorr 302). App Links al redirect from a we mobile app. If this incorrectly config Link host/domain can hijack such U to phishing attack data in the URI, su tokens, magic link tokens and more. App Link domain assetlinks.json fil verification via [android:autoVeri Activity intent-filt

NO	ISSUE	SEVERITY	DESCRIPTION
7	App Link assetlinks.json file not found [android:name=com.united.mobile.android.ui.main.MainActivity] [android:host=http://click.enews.united.com]	high	App Link asset ve (http://click.enew known/assetlinks configured incorr 301). App Links al redirect from a we mobile app. If this incorrectly config Link host/domain can hijack such U to phishing attack data in the URI, su tokens, magic link tokens and more. App Link domain assetlinks.json fil verification via [android:autoVeri Activity intent-filt
8	**Activity** (com.united.mobile.android.ui.main.MainActivity) is not Protected. [android:exported=true]	warning	An Activity is foun other apps on the leaving it accessib application on the

NO	ISSUE	SEVERITY	DESCRIPTION
9	**Activity-Alias** (com.united.mobile.android.ui.main.TravelReadyCenterAlias) is not Protected. [android:exported=true]	warning	An Activity-Alias is shared with other therefore leaving other application
10	**Broadcast Receiver** (com.united.mobile.android.widget.tripCountDown.TripCountDownWidgetLargeProvider) is Protected by a permission, but the protection level of the permission should be checked. **Permission:** com.united.mobile.android.Main [android:exported=true]	warning	A Broadcast Recei shared with other therefore leaving other application protected by a pe not defined in the application. As a r protection level o should be checke defined. If it is set dangerous, a mali can request and c permission and ir component. If it is only applications same certificate c permission.

Showing 1 to 10 of 19 entries

Previous 1 2 Next

</> CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SUPPRESSED
7	9	3	2	0

Search:

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTION
1	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		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTION
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		
3	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	**CWE:** CWE-749: Exposed Dangerous Method or Function **OWASP Top 10:** M1: Improper Platform Usage **OWASP MASVS:** MSTG-PLATFORM-7		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTION
4	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		
5	App can write to App Directory. Sensitive Information should be encrypted.	info	**CWE:** CWE-276: Incorrect Default Permissions **OWASP MASVS:** MSTG-STORAGE-14		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTION
6	Remote WebView debugging is enabled.	high	**CWE:** CWE-919: Weaknesses in Mobile Applications **OWASP Top 10:** M1: Improper Platform Usage **OWASP MASVS:** MSTG-RESILIENCE-2	com/united/mobile/android/game/ui/fsim/GameMainActivity.java com/united/mobile/android/game/ui/santassleigh/GameSantaActivity.java	
7	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	**OWASP MASVS:** MSTG-NETWORK-4		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTION
8	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		
9	App creates temp file. Sensitive information should never be written into a temp file.	warning	**CWE:** CWE-276: Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTION
10	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		

Showing 1 to 10 of 21 entries

Previous 1 2 3 Next

SHARED LIBRARY BINARY ANALYSIS

Search:

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY
1	x86/libnative-lib.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY
2	x86/libcpuinfo.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY
3	x86/libc++_shared.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY
4	x86/libBlinkCard.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY
5	x86/libLIB-v.4.3.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY
6	x86/libnode.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**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.	**No RELRO** high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to	**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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY
				enable full RELRO and only -z,relro to enable partial RELRO.			

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY
7	x86/libmapbox-gl.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY
8	arm64-v8a/libnative-lib.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY
9	arm64-v8a/libaleInterface.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**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: ['__strlen_chk', '__vsnprintf_chk', '__vsprintf_chk', '__read_chk', '__memmove_chk']

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY
10	arm64-v8a/libcpuinfo.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**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: ['__read_chk']

Showing 1 to 10 of 82 entries

Previous 1 2 3 4 5 … 9 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
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

APKiD ANALYSIS

Search:

DEX	DETECTIONS
classes.dex	Search:

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check
Compiler	unknown (please file detection issue!)
yara_issue	yara issue - dex file recognized by apkid but not yara module

Showing 1 to 3 of 3 entries

Previous 1 Next

DEX	DETECTIONS
classes10.dex	

Search:

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check possible Build.SERIAL check network operator name check
Compiler	unknown (please file detection issue!)
yara_issue	yara issue - dex file recognized by apkid but not yara module

Showing 1 to 3 of 3 entries

Previous 1 Next

DEX	DETECTIONS
classes11.dex	

Search:

FINDINGS	DETAILS
Anti-VM Code	Build.MODEL check Build.PRODUCT check possible VM check
Compiler	unknown (please file detection issue!)
yara_issue	yara issue - dex file recognized by apkid but not yara module

Showing 1 to 3 of 3 entries

Previous 1 Next

DEX	DETECTIONS
classes2.dex	

Search:

FINDINGS	DETAILS
Anti Disassembly Code	illegal class name
Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.BOARD check
Compiler	unknown (please file detection issue!)
yara_issue	yara issue - dex file recognized by apkid but not yara module

Showing 1 to 4 of 4 entries

Previous 1 Next

DEX	DETECTIONS
classes3.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 Build.TAGS check
Compiler	unknown (please file detection issue!)
yara_issue	yara issue - dex file recognized by apkid but not yara module

Showing 1 to 3 of 3 entries

Previous 1 Next

DEX	DETECTIONS
classes4.dex	

Search:

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.BOARD check Build.TAGS check SIM operator check network operator name check
Compiler	unknown (please file detection issue!)
yara_issue	yara issue - dex file recognized by apkid but not yara module

Showing 1 to 3 of 3 entries

Previous 1 Next

DEX	DETECTIONS
classes5.dex	

Search:

FINDINGS	DETAILS
Anti Debug Code	Debug.isDebuggerConnected() check
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible Build.SERIAL check network operator name check ro.kernel.qemu check
Compiler	unknown (please file detection issue!)
yara_issue	yara issue - dex file recognized by apkid but not yara module

Showing 1 to 4 of 4 entries

Previous 1 Next

DEX	DETECTIONS
classes6.dex	Search:

FINDINGS	DETAILS
Compiler	unknown (please file detection issue!)
yara_issue	yara issue - dex file recognized by apkid but not yara module

Showing 1 to 2 of 2 entries

Previous 1 Next

DEX	DETECTIONS
classes7.dex	Search:

FINDINGS	DETAILS
Compiler	unknown (please file detection issue!)
yara_issue	yara issue - dex file recognized by apkid but not yara module

Showing 1 to 2 of 2 entries

Previous 1 Next

DEX	DETECTIONS
classes8.dex	Search:

FINDINGS	DETAILS
Anti-VM Code	Build.PRODUCT check
Compiler	unknown (please file detection issue!)
yara_issue	yara issue - dex file recognized by apkid but not yara module

Showing 1 to 3 of 3 entries

Previous 1 Next

Showing 1 to 10 of 13 entries

Previous 1 2 Next

QUARK ANALYSIS

Search:

POTENTIAL MALICIOUS BEHAVIOUR	EVIDENCE
No data available in table	

Showing 0 to 0 of 0 entries

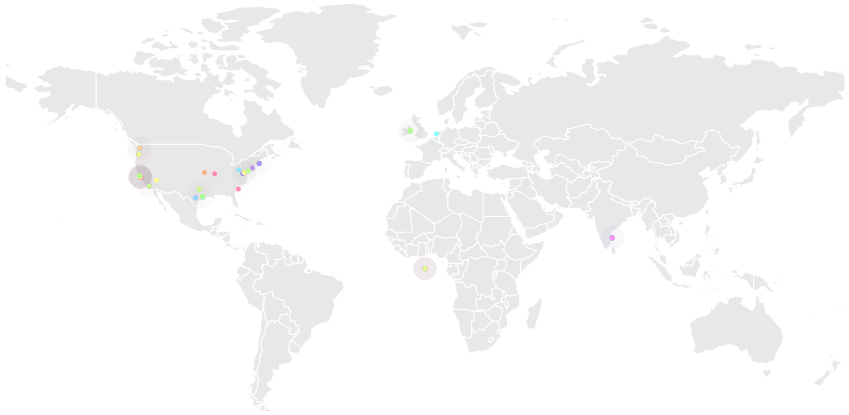
Previous Next

ABUSED PERMISSIONS

Top Malware Permissions	14/24	Other Common Permissions
android.permission.INTERNET, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.SYSTEM_ALERT_WINDOW, android.permission.VIBRATE, android.permission.CAMERA, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.READ_PHONE_STATE, android.permission.RECORD_AUDIO, android.permission.RECEIVE_BOOT_COMPLETED		android.permission.READ_CALENDAR, android.permission.CALL_PHON android.permission.FOREGROUND_SERVICE, android.permission.CHANGE_WIFI_STATE, android.permission.BLUETC android.permission.BLUETOOTH_ADMIN, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.FLASHLIGHT, com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER

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
192.168.1.25	ok	**IP:** 192.168.1.25 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
192.168.1.3	ok	**IP:** 192.168.1.3 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
1s-app.quantummetric.com	ok	**IP:** 34.27.112.206 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
ad.doubleclick.net	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
adroit-nectar-425.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
airborne.inflightinternet.com	ok	No Geolocation information available.
airbornemedia.inflightinternet.com	ok	No Geolocation information available.
ajaxgeo.cartrawler.com	ok	**IP:** 64.12.0.90 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.731323 **Longitude:** -73.990089 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

Showing 1 to 10 of 183 entries

Previous 1 2 3 4 5 … 19 Next

URLS

Search:

URL	FILE
data::class.java	com/united/mobile/android/reservation/ui/seatmap/upgradeseat/UpgradeSeatViewModel.
data::class.java)	com/united/mobile/android/flightstatus/repository/PCUSharedRepositoryImpl.java
data::class.java)	com/united/mobile/android/booking/ui/editSearch/EditSearchViewModel.java
data::class.java)	cartrawler/core/di/providers/SessionDataModule.java

URL	FILE
data::class.java.name	com/united/mobile/android/checkin/comm/NavigationObject.java
data::init(const http://rarepixels.com/apps/planes-control/privacy/ data::addsample(const http://www.apple.com/dtds/propertylist-1.0.dtd https://twitter.com/planes_control https://www.facebook.com/planesapp	apktool_out/lib/arm64-v8a/libMyGame.so
data::init(const http://rarepixels.com/apps/planes-control/privacy/ data::addsample(const http://www.apple.com/dtds/propertylist-1.0.dtd https://twitter.com/planes_control https://www.facebook.com/planesapp	lib/arm64-v8a/libMyGame.so
data:image	com/bumptech/glide/load/model/DataUrlLoader.java
	com/united/mobile/android/bagtracking/utility/FragmentUtilsKt.java
file:///android_asset/	com/bumptech/glide/load/model/AssetUriLoader.java

Showing 1 to 10 of 183 entries

Previous 1 2 3 4 5 … 19 Next

FIREBASE DATABASE

Search:

FIREBASE URL	DETAILS
https://adroit-nectar-425.firebaseio.com	info App talks to a Firebase database.

Showing 1 to 1 of 1 entries

Previous 1 Next

EMAILS

Search:

EMAIL	FILE
8rf@oa3.0j99	com/inmobile/iiivvv.java
carhire-excess@axa-assistance.co games@united.com emailaddress@gmail.com	Android String Resource

EMAIL	FILE
contact@rarepixels.com	apktool_out/lib/arm64-v8a/libMyGame.so
contact@rarepixels.com	lib/arm64-v8a/libMyGame.so
devsupport@getgrab.com	com/locuslabs/sdk/llprivate/GrabController.java
kmjones3@gmail.com	com/united/mobile/android/checkin/service/MockCheckInServiceImpl.java
lynethpeou2003@hotmail.com brussell@example.com	com/united/mobile/android/checkin/utils/CheckInMockDataSource.java
wifi@united.com	com/united/mobile/android/unifiedplayer/repository/unifiedplayer/Constants.java

Showing 1 to 8 of 8 entries

Previous 1 Next

TRACKERS

Search:

TRACKER NAME	CATEGORIES	URL
Button	Analytics, Profiling, Identification	https://reports.exodus-privacy.eu.org/trackers/340
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312

TRACKER NAME	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Inmobi		https://reports.exodus-privacy.eu.org/trackers/106
Kochava	Analytics, Profiling, Advertisement	https://reports.exodus-privacy.eu.org/trackers/127
Locuslabs		https://reports.exodus-privacy.eu.org/trackers/60
Qualtrics		https://reports.exodus-privacy.eu.org/trackers/306
Snowplow	Analytics	https://reports.exodus-privacy.eu.org/trackers/108

Showing 1 to 8 of 8 entries

Previous 1 Next

POSSIBLE HARDCODED SECRETS

▶ Show all **641** secrets

STRINGS

From APK Resource

▶ Show all **69545** strings

From Code

▶ Show all **156775** strings

From Shared Objects

apktool_out/lib/x86/libnative-lib.so

▼ Showing all **3** strings
LogNode
Couldn't start redirecting stdout and stderr to logcat.
NODE_PATH

apktool_out/lib/x86/libcpuinfo.so

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

apktool_out/lib/x86/libc++_shared.so

▶ Show all **560** strings

apktool_out/lib/x86/libBlinkCard.so

▶ Show all **4457** strings

apktool_out/lib/x86/libLIB-v.4.3.so

▶ Show all **359** strings

apktool_out/lib/x86/libnode.so

▶ Show all **24714** strings

apktool_out/lib/x86/libmapbox-gl.so

▶ Show all **4896** strings

apktool_out/lib/arm64-v8a/libnative-lib.so

▼ Showing all **3** strings

LogNode
Couldn't start redirecting stdout and stderr to logcat.
NODE_PATH

apktool_out/lib/arm64-v8a/libaleInterface.so

▶ Show all **1672** strings

apktool_out/lib/arm64-v8a/libcpuinfo.so

▶ Show all **5** strings

apktool_out/lib/arm64-v8a/libc++_shared.so

▶ Show all **643** strings

apktool_out/lib/arm64-v8a/libBlinkCard.so

▶ Show all **4352** strings

apktool_out/lib/arm64-v8a/libLIB-v.4.3.so

▶ Show all **338** strings

apktool_out/lib/arm64-v8a/libJVCardFindJava.so

▶ Show all **346** strings

apktool_out/lib/arm64-v8a/libnode.so

▶ Show all **21319** strings

apktool_out/lib/arm64-v8a/libJVImgJava.so

▶ Show all **61** strings

apktool_out/lib/arm64-v8a/libJVCoreJava.so

▶ Show all **79** strings

apktool_out/lib/arm64-v8a/libJVMrzJava.so

▶ Show all **966** strings

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

▶ Show all **4940** strings

apktool_out/lib/arm64-v8a/libJVCore.so

▶ Show all **2908** strings

apktool_out/lib/arm64-v8a/libMyGame.so

▶ Show all **4829** strings

apktool_out/lib/armeabi-v7a/libnative-lib.so

▼ Showing all **3** strings

LogNode

Couldn't start redirecting stdout and stderr to logcat.

NODE_PATH

apktool_out/lib/armeabi-v7a/libaleInterface.so

▶ Show all **1671** strings

apktool_out/lib/armeabi-v7a/libcpuinfo.so

▶ Show all **22** strings

apktool_out/lib/armeabi-v7a/libc++_shared.so

▶ Show all **639** strings

apktool_out/lib/armeabi-v7a/libBlinkCard.so

▶ Show all **4472** strings

apktool_out/lib/armeabi-v7a/libLIB-v.4.3.so

▶ Show all **387** strings

apktool_out/lib/armeabi-v7a/libJVCardFindJava.so

▶ Show all **308** strings

apktool_out/lib/armeabi-v7a/libnode.so

▶ Show all **20006** strings

apktool_out/lib/armeabi-v7a/libJVImgJava.so

▶ Show all **42** strings

apktool_out/lib/armeabi-v7a/libJVCoreJava.so

▶ Show all **61** strings

apktool_out/lib/armeabi-v7a/libJVMrzJava.so

▶ Show all **923** strings

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

▶ Show all **4926** strings

apktool_out/lib/armeabi-v7a/libJVCore.so

▶ Show all **2910** strings

apktool_out/lib/x86_64/libnative-lib.so

▼ Showing all **3** strings

LogNode

Couldn't start redirecting stdout and stderr to logcat.

NODE_PATH

apktool_out/lib/x86_64/libcpuinfo.so

▼ Showing all **3** strings

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

apktool_out/lib/x86_64/libc++_shared.so

▶ Show all **566** strings

apktool_out/lib/x86_64/libBlinkCard.so

▶ Show all **4779** strings

apktool_out/lib/x86_64/libLIB-v.4.3.so

▶ Show all **361** strings

apktool_out/lib/x86_64/libnode.so

▶ Show all **24921** strings

apktool_out/lib/x86_64/libmapbox-gl.so

▶ Show all **4903** strings

lib/x86/libnative-lib.so

▼ Showing all **3** strings
LogNode
Couldn't start redirecting stdout and stderr to logcat.
NODE_PATH

lib/x86/libcpuinfo.so

▼ Showing all **3** strings

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

lib/x86/libc++_shared.so

▶ Show all **560** strings

lib/x86/libBlinkCard.so

▶ Show all **4457** strings

lib/x86/libLIB-v.4.3.so

▶ Show all **359** strings

lib/x86/libnode.so

▶ Show all **24714** strings

lib/x86/libmapbox-gl.so

▶ Show all **4896** strings

lib/arm64-v8a/libnative-lib.so

▼ Showing all **3** strings

LogNode
Couldn't start redirecting stdout and stderr to logcat.
NODE_PATH

lib/arm64-v8a/libaleInterface.so

▶ Show all **1672** strings

lib/arm64-v8a/libcpuinfo.so

▶ Show all **5** strings

lib/arm64-v8a/libc++_shared.so

▶ Show all **643** strings

lib/arm64-v8a/libBlinkCard.so

▶ Show all **4352** strings

lib/arm64-v8a/libLIB-v.4.3.so

▶ Show all **338** strings

lib/arm64-v8a/libJVCardFindJava.so

▶ Show all **346** strings

lib/arm64-v8a/libnode.so

▶ Show all **21319** strings

lib/arm64-v8a/libJVImgJava.so

▶ Show all **61** strings

lib/arm64-v8a/libJVCoreJava.so

▶ Show all **79** strings

lib/arm64-v8a/libJVMrzJava.so

▶ Show all **966** strings

lib/arm64-v8a/libmapbox-gl.so

▶ Show all **4940** strings

lib/arm64-v8a/libJVCore.so

▶ Show all **2908** strings

lib/arm64-v8a/libMyGame.so

▶ Show all **4829** strings

lib/armeabi-v7a/libnative-lib.so

▼ Showing all **3** strings

LogNode

Couldn't start redirecting stdout and stderr to logcat.

NODE_PATH

lib/armeabi-v7a/libaleInterface.so

▶ Show all **1671** strings

lib/armeabi-v7a/libcpuinfo.so

▶ Show all **22** strings

lib/armeabi-v7a/libc++_shared.so

▶ Show all **639** strings

lib/armeabi-v7a/libBlinkCard.so

▶ Show all **4472** strings

lib/armeabi-v7a/libLIB-v.4.3.so

▶ Show all **387** strings

lib/armeabi-v7a/libJVCardFindJava.so

▶ Show all **308** strings

lib/armeabi-v7a/libnode.so

▶ Show all **20006** strings

lib/armeabi-v7a/libJVImgJava.so

▶ Show all **42** strings

lib/armeabi-v7a/libJVCoreJava.so

▶ Show all **61** strings

lib/armeabi-v7a/libJVMrzJava.so

▶ Show all **923** strings

lib/armeabi-v7a/libmapbox-gl.so

▶ Show all **4926** strings

lib/armeabi-v7a/libJVCore.so

▶ Show all **2910** strings

lib/x86_64/libnative-lib.so

▼ Showing all **3** strings
LogNode
Couldn't start redirecting stdout and stderr to logcat.
NODE_PATH

lib/x86_64/libcpuinfo.so

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

lib/x86_64/libc++_shared.so

▶ Show all **566** strings

lib/x86_64/libBlinkCard.so

▶ Show all **4779** strings

lib/x86_64/libLIB-v.4.3.so

▶ Show all **361** strings

lib/x86_64/libnode.so

▶ Show all **24921** strings

lib/x86_64/libmapbox-gl.so

▶ Show all **4903** strings

ACTIVITIES

▼ Showing all **33** activities

com.united.mobile.android.ui.splash.SplashActivity
com.united.mobile.android.ui.NfcActivity
com.united.mobile.android.ui.main.MainActivity
com.jumio.nv.NetverifyActivity
com.qualtrics.digital.QualtricsSurveyActivity
com.qualtrics.digital.QualtricsPopOverActivity
com.united.mobile.android.game.ui.fsim.GameMainActivity
com.united.mobile.android.game.ui.santassleigh.GameSantaActivity
org.cocos2dx.cpp.AppActivity
com.united.mobile.android.unifiedplayer.repository.unifiedplayer.UnifiedPlayerActivity
com.liveperson.infra.messaging_ui.ConversationActivity
cartrawler.core.ui.modules.payment.options.googlepay.GooglePayTokenActivity
cartrawler.core.base.CartrawlerActivity
com.liveperson.lpdatepicker.DatePickerActivity
com.microblink.blinkcard.activity.BlinkCardActivity
com.microblink.blinkcard.activity.edit.BlinkCardEditActivity
androidx.biometric.DeviceCredentialHandlerActivity
com.uplift.sdk.offer.ui.view.OfferActivity
com.uplift.sdk.checkout.ui.view.CheckoutActivity
com.google.android.gms.common.api.GoogleApiActivity

com.journeyapps.barcodescanner.CaptureActivity
com.google.android.gms.ads.AdActivity
com.google.android.gms.ads.OutOfContextTestingActivity
com.google.android.gms.ads.NotificationHandlerActivity
com.usebutton.sdk.internal.InstallCardActivity
com.usebutton.sdk.internal.GroupedInventoryCardActivity
com.usebutton.sdk.internal.SingleProductCardActivity
com.usebutton.sdk.internal.WebViewActivity
com.usebutton.sdk.internal.AuthChallengeActivity
com.usebutton.sdk.internal.InstallSheetActivity
com.google.android.play.core.missingsplits.PlayCoreMissingSplitsActivity
com.google.android.play.core.common.PlayCoreDialogWrapperActivity
com.qualtrics.digital.QualtricsEmbeddedFeedbackActivity

SERVICES

▼ Showing all **19** services
com.united.mobile.android.checkin.ui.main.pinning.CheckInMbpPinningService
com.united.mobile.android.widget.tripCountDown.TripCountDownWidgetService
com.united.mobile.android.firebase.FcmJobService
com.united.mobile.android.firebase.LiveActivityService
com.united.mobile.android.firebase.FcmMessageService
com.liveperson.infra.messaging_ui.utils.ConversationInBackgroundService
com.liveperson.messaging.background.BackgroundActionsService
com.google.firebase.messaging.FirebaseMessagingService
com.google.firebase.components.ComponentDiscoveryService
com.google.android.gms.ads.AdService
androidx.work.impl.background.systemalarm.SystemAlarmService

androidx.work.impl.background.systemjob.SystemJobService
androidx.work.impl.foreground.SystemForegroundService
androidx.room.MultiInstanceInvalidationService
com.google.android.datatransport.runtime.backends.TransportBackendDiscovery
com.google.android.datatransport.runtime.scheduling.jobscheduling.JobInfoSchedulerService
com.google.android.play.core.assetpacks.AssetPackExtractionService
com.google.android.play.core.assetpacks.ExtractionForegroundService
com.inmobile.IsolatedService

RECEIVERS

▼ Showing all **17** receivers
com.united.mobile.android.widget.tripCountDown.TripCountDownWidgetLargeProvider
com.united.mobile.android.ui.main.notification.NotificationReceiver
com.united.mobile.android.appcore.receiver.InstallReferrerReceiver
com.appsamurai.storyly.util.notification.StorylyNotificationReceiver
com.google.firebase.iid.FirebaseInstanceIdReceiver
com.usebutton.sdk.internal.receivers.LocaleChangedReceiver
com.usebutton.sdk.internal.receivers.InstallNotificationReceiver
androidx.work.impl.utils.ForceStopRunnable$BroadcastReceiver
androidx.work.impl.background.systemalarm.ConstraintProxy$BatteryChargingProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$BatteryNotLowProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$StorageNotLowProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$NetworkStateProxy
androidx.work.impl.background.systemalarm.RescheduleReceiver
androidx.work.impl.background.systemalarm.ConstraintProxyUpdateReceiver
androidx.work.impl.diagnostics.DiagnosticsReceiver

com.google.android.datatransport.runtime.scheduling.jobscheduling.AlarmManagerSchedulerBroadcastReceiver
com.qualtrics.digital.QualtricsNotificationManager

PROVIDERS

▼ Showing all **11** providers
com.united.mobile.android.reservation.model.ReservationFileProvider
com.united.mobile.android.commonui.model.commonwebview.CommonUIFileProvider
com.liveperson.infra.messaging_ui.utils.LpFileProvider
com.liveperson.messaging.wm.WelcomeMessageContentProvider
com.liveperson.infra.utils.LPInitProvider
com.uplift.sdk.util.UpliftFileProvider
com.google.firebase.provider.FirebaseInitProvider
com.google.android.gms.ads.MobileAdsInitProvider
androidx.startup.InitializationProvider
com.squareup.picasso.PicassoProvider
com.inmobile.MeshProvider

LIBRARIES

▼ Showing all **4** libraries
org.apache.http.legacy
android.ext.adservices
androidx.window.extensions
androidx.window.sidecar

FILES

▶ Show all **8471** files

 Version v3.9.8 Beta