

MASVS-PLATFORM-1:

App Permissions:

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
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.

For permissions the app uses most of them with in reason such as location, wifi, and bluetooth. Although why it needs bluetooth permissions is unknown at the moment. The most concerning permissions however are the ad permissions that reduce user privacy and of most concern a custom permisison to allow connection to inflight panasonic devices.

Testing for Sensitive Functionality Exposure through IPC:

The following reported exported as true:

```
<activity android:theme="@android:style/Theme.NoDisplay"
android:name="com.united.mobile.android.ui.NfcActivity" android:exported="true">

<activity android:name="com.united.mobile.android.ui.main.MainActivity" android:exported="true"
android:launchMode="singleTask" android:configChanges="screenSize|orientation">

<activity-alias android:name="com.united.mobile.android.ui.main.TravelReadyCenterAlias"
android:exported="true" android:targetActivity="com.united.mobile.android.ui.main.MainActivity">

<receiver android:name="com.united.mobile.android.widget.tripCountDown.TripCountDownWidgetLargeProvider"
android:permission="com.united.mobile.android.Main" android:enabled="true" android:exported="true">

<activity-alias android:name="com.united.mobile.android.ui.main.TravelReadyCenterAlias"
android:exported="true" android:targetActivity="com.united.mobile.android.ui.main.MainActivity">

<receiver android:name="com.united.mobile.android.appcore.receiver.InstallReferrerReceiver"
android:enabled="true" android:exported="true">

<activity android:theme="@style/DeviceCredentialHandlerTheme"
android:name="androidx.biometric.DeviceCredentialHandlerActivity" android:exported="true"/>

<receiver android:name="com.google.firebase.iid.FirebaseInstanceIdReceiver"
android:permission="com.google.android.c2dm.permission.SEND" android:exported="true">

<receiver android:name="com.usebutton.sdk.internal.receivers.LocaleChangedReceiver"
android:exported="true">

<service android:name="androidx.work.impl.background.systemjob.SystemJobService"
android:permission="android.permission.BIND_JOB_SERVICE"
android:enabled="@bool/enable_system_job_service_default" android:exported="true"
android:directBootAware="false"/>

<receiver android:name="androidx.work.impl.diagnostics.DiagnosticsReceiver"
android:permission="android.permission.DUMP" android:enabled="true" android:exported="true"
android:directBootAware="false">
<service android:name="com.google.android.play.core.assetpacks.AssetPackExtractionService"
android:enabled="false" android:exported="true">

<provider android:name="com.inmobile.MeshProvider" android:readPermission="" android:enabled="true"
android:exported="true" android:authorities="com.united.mobile.android.provider" android:syncable="true"/>
```

App also has many intent filters:

```
<intent-filter>
    <action android:name="android.intent.action.VIEW"/>
</intent-filter>
<intent-filter android:autoVerify="true">
    <action android:name="android.intent.action.VIEW"/>
    <category android:name="android.intent.category.DEFAULT"/>
    <category android:name="android.intent.category.BROWSABLE"/>
    <data android:scheme="http"/>
    <data android:scheme="https"/>
    <data android:host="www.united.com"/>
    <data android:host="united.com"/>
    <data android:pathPrefix="/ual/en/us/navigation/airportna"/>
    <data android:pathPrefix="/ual/en/us/navigation/airportNA"/>
    <data android:pathPrefix="/ual/en/US/navigation/airportna"/>
    <data android:pathPrefix="/ual/en/US/navigation/airportNA"/>
    <data android:pathPrefix="/en/us/fly/travel/airport/termi"/>
</intent-filter>
<intent-filter android:autoVerify="true">
    <action android:name="android.intent.action.VIEW"/>
    <category android:name="android.intent.category.BROWSABLE"/>
    <category android:name="android.intent.category.DEFAULT"/>
    <data android:scheme="ualentertainment"/>
</intent-filter>
<intent-filter android:autoVerify="true">
    <action android:name="android.intent.action.VIEW"/>
    <category android:name="android.intent.category.BROWSABLE"/>
    <category android:name="android.intent.category.DEFAULT"/>
    <data android:scheme="ualpartnerprovisionreturn"/>
    <data android:scheme="ualpartnerprovisioncancel"/>
</intent-filter>
<intent-filter android:autoVerify="true">
    <action android:name="android.intent.action.VIEW"/>
    <category android:name="android.intent.category.BROWSABLE"/>
    <category android:name="android.intent.category.DEFAULT"/>
    <data android:scheme="http"/>
    <data android:scheme="https"/>
    <data android:host="www.united.com"/>
    <data android:host="united.com"/>
    <data android:host="news.united.com"/>
    <data android:pathPrefix="/offers/myoffers"/>
</intent-filter>
<intent-filter android:autoVerify="true">
    <action android:name="android.intent.action.VIEW"/>
    <category android:name="android.intent.category.BROWSABLE"/>
    <category android:name="android.intent.category.DEFAULT"/>
    <data android:scheme="ualpaypalreturn"/>
    <data android:scheme="ualpaypalcancel"/>
</intent-filter>
<intent-filter android:autoVerify="true">
    <action android:name="android.intent.action.VIEW"/>
```

Testing Deep Links:

com.united.mobile.android.ui.NfcActivity

- `unitednfctag://nfcbagprint`

com.united.mobile.android.ui.main.MainActivity

- <http://click.ews.united.com/>
- <http://news.united.com/offers/myoffers>
- <http://news.united.com/pub/acc>
- <http://united.com/en/US/managers/tripdetails>
- <http://united.com/en/us/account>
- <http://united.com/en/us/checkin>
- <http://united.com/en/us/flightstatus/details>
- <http://united.com/en/us/fly/travel/airport/terminal-guide/download-app.html>
- <http://united.com/en/us/fly/travel/mobile-tools/united-trip-planner>
- <http://united.com/en/us/manageRes/tripDetails>
- <http://united.com/en/us/managers/tripdetails>
- <http://united.com/offers/myoffers>
- <http://united.com/s/us>
- <http://united.com/travel/checkin/quickstart>
- <http://united.com/ual/en/US/navigation/airportNAV/nav>
- <http://united.com/ual/en/US/navigation/airportnav/nav>
- <http://united.com/ual/en/us/navigation/airportNAV/nav>
- <http://united.com/ual/en/us/navigation/airportnav/nav>
- <http://www.united.com/en-us/flights>
- <http://www.united.com/en/US/managers/tripdetails>
- <http://www.united.com/en/us/account>
- <http://www.united.com/en/us/checkin>
- <http://www.united.com/en/us/flightstatus/details>
- <http://www.united.com/en/us/fly/travel/airport/terminal-guide/download-app.html>
- <http://www.united.com/en/us/fly/travel/mobile-tools/united-trip-planner>
- <http://www.united.com/en/us/manageRes/tripDetails>
- <http://www.united.com/en/us/managers/mytrips>
- <http://www.united.com/en/us/managers/tripdetails>
- <http://www.united.com/offers/myoffers>
- <http://www.united.com/s/us>
- <http://www.united.com/travel/checkin/quickstart>
- <http://www.united.com/ual/en/US/navigation/airportNAV/nav>
- <http://www.united.com/ual/en/US/navigation/airportnav/nav>
- <http://www.united.com/ual/en/us/navigation/airportNAV/nav>

- <http://www.united.com/ual/en/us/navigation/airportnav/nav>
- <http://www.unitedwifi.com/portal/V/appdetection>
- <https://click.enuws.united.com/>
- <https://news.united.com/offers/myoffers>
- <https://news.united.com/pub/acc>
- <https://united.com/en/US/manageres/tripdetails>
- <https://united.com/en/us/account>
- <https://united.com/en/us/baggage/issues-with-your-checked-bags>
- <https://united.com/en/us/checkin>
- <https://united.com/en/us/digital-wallet/checkout>
- <https://united.com/en/us/flightstatus/details>
- <https://united.com/en/us/fly/travel/airport/terminal-guide/download-app.html>
- <https://united.com/en/us/fly/travel/baggage/tracking>
- <https://united.com/en/us/fly/travel/mobile-tools/united-trip-planner>
- <https://united.com/en/us/manageRes/tripDetails>
- <https://united.com/en/us/manageres/tripdetails>
- <https://united.com/en/us/myunited/verify/email>
- <https://united.com/en/us/myunited/verify/phone>
- <https://united.com/en/us/pbs>
- <https://united.com/en/us/preordermeals/deeplink/marketing>
- <https://united.com/en/us/preordermeals/flightinformation>
- <https://united.com/en/us/travelreadycenter>
- <https://united.com/offers/myoffers>
- <https://united.com/s/us>
- <https://united.com/travel/checkin/quickstart>
- <https://united.com/travelreadycenter>
- <https://united.com/ual/en/US/navigation/airportNAV/nav>
- <https://united.com/ual/en/US/navigation/airportnav/nav>
- <https://united.com/ual/en/us/navigation/airportNAV/nav>
- <https://united.com/ual/en/us/navigation/airportnav/nav>
- <https://www.united.com/Booking/SearchInjection/VendorQueryPinDown>
- <https://www.united.com/en-us/flights>
- <https://www.united.com/en/US/manageres/tripdetails>
- <https://www.united.com/en/us/account>
- <https://www.united.com/en/us/baggage/issues-with-your-checked-bags>
- <https://www.united.com/en/us/checkin>

- <https://www.united.com/en/us/digital-wallet/checkout>
- <https://www.united.com/en/us/flightstatus/details>
- <https://www.united.com/en/us/fly/print/bagtag>
- <https://www.united.com/en/us/fly/travel/airport/terminal-guide/download-app.html>
- <https://www.united.com/en/us/fly/travel/baggagepacking>
- <https://www.united.com/en/us/fly/travel/mobile-tools/united-trip-planner>
- <https://www.united.com/en/us/manageRes/tripDetails>
- <https://www.united.com/en/us/managers/mytrips>
- <https://www.united.com/en/us/managers/tripdetails>
- <https://www.united.com/en/us/myunited/verify/email>
- <https://www.united.com/en/us/myunited/verify/phone>
- <https://www.united.com/en/us/pbs>
- <https://www.united.com/en/us/preordermeals/deep-link/marketing>
- <https://www.united.com/en/us/preordermeals/flight-information>
- <https://www.united.com/en/us/travelreadycenter>
- <https://www.united.com/offers/myoffers>
- <https://www.united.com/s/us>
- <https://www.united.com/travel/checkin/quickstart>

All united related links I deemed to be legitimate

- <https://www.united.com/travelreadycenter>
- <https://www.united.com/ual/en/US/navigation/airportNAV/nav>
- <https://www.united.com/ual/en/US/navigation/airportnav/nav>
- <https://www.united.com/ual/en/jp/Booking/SearchInjection/VendorQueryPinDown>
- <https://www.united.com/ual/en/us/Booking/SearchInjection/VendorQueryPinDown>
- <https://www.united.com/ual/en/us/navigation/airportNAV/nav>
- <https://www.united.com/ual/en/us/navigation/airportnav/nav>
- <https://www.unitedwifi.com/portal/l/appdetection>
- <https://www.unitedwifi.com/portal/vod/playmovie>
- [ualentertainment://](#)
- [ualmasterpassreturn://](#)
- [ualmobile://flights](#)
- [ualmobile://homescreen](#)
- [ualmobile://mytrips](#)
- [ualmobile://openapp/*](#)
- [ualpartnerprovisioncancel://](#)
- [ualpartnerprovisionreturn://](#)
- [ualpaypalcancel://](#)
- [ualpaypalreturn://](#)
- [ualprepaidbagsreturn://](#)
- [uaportalpacstream://](#)

MASVS-PLATFORM-2:

Testing Javascript Execution in WebViews:

```

m com.usebutton.sdk.internal.views.PopupWebView.initP webView.getSettings().setJavaScriptEnabled(true);
m com.usebutton.sdk.internal.views.OverlayWebView.init observableWebView.getSettings().setJavaScriptEnabled(
m com.google.ads.interactivemedia.v3.internal.agv.j() webView.getSettings().setJavaScriptEnabled(true);
m com.google.ads.interactivemedia.v3.internal.ajm.ajm webView.getSettings().setJavaScriptEnabled(true);
m com.google.android.gms.internal.ads.zzfmo.zzk() void webView.getSettings().setJavaScriptEnabled(true);
m com.google.ads.interactivemedia.v3.internal.agt.agt webView.getSettings().setJavaScriptEnabled(true);
m com.google.android.gms.internal.ads.zzfml.zzfml(Web webView.getSettings().setJavaScriptEnabled(true);
m com.united.mobile.android.homescreen.ui.travelcenter this.webView.getSettings().setJavaScriptEnabled(true)
m com.google.ads.interactivemedia.v3.internal.aip.aip getSettings().setJavaScriptEnabled(true);
m com.united.mobile.android.commonui.model.commonwebvi this.webView.getSettings().setJavaScriptEnabled(true)
m org.cocos2dx.lib.Cocos2dxWebView.Cocos2dxWebView(Cor getSettings().setJavaScriptEnabled(true);
m com.google.android.gms.internal.consent_sdk.zzbe.zzb zzb.getSettings().setJavaScriptEnabled(true);
m com.united.mobile.android.commonui.view.commonwebvi this.webView.getSettings().setJavaScriptEnabled(true)
m com.quantummetric.instrument.aw.aw(WebView, aw$a) vc webView.getSettings().setJavaScriptEnabled(true);
m com.google.android.gms.ads.internal.zzs.zzs(Context, this.zzf.getSettings().setJavaScriptEnabled(true);
m com.qualtrics.digital.QualtricsSurveyFragment.onCreate this.webView.getSettings().setJavaScriptEnabled(true)
m com.uplift.sdk.util.web.BaseWebView.a(WDDispatcher) \ settings.setJavaScriptEnabled(true);
m com.jumio.sdk.views.JumioDigitalIdentityView.JumioDi settings.setJavaScriptEnabled(true);
m com.jumio.sdk.views.JumioDigitalIdentityView.JumioDi settings.setJavaScriptEnabled(true);
m com.google.android.gms.internal.ads.zzcho.zzcho(zzcj settings.setJavaScriptEnabled(true);
m com.usebutton.sdk.internal.WebViewActivity.configure settings.setJavaScriptEnabled(true);
m com.united.mobile.android.game.ui.fsim.GameMainActiv settings.setJavaScriptEnabled(true);
m com.united.mobile.android.game.ui.santassleigh.GameS settings.setJavaScriptEnabled(true);
m com.united.mobile.android.game.ui.trivia.implementat webView.getSettings().setJavaScriptEnabled(true);
m com.united.mobile.android.checkin.ui.webView.CheckIr this.webView.getSettings().setJavaScriptEnabled(true)
m cartrawler.core.ui.modules.webview.WebViewFragment.k settings.setJavaScriptEnabled(true);
m com.quantummetric.instrument.av.a(av, Context) void avVar.f4539b.getSettings().setJavaScriptEnabled(true)
m com.united.mobile.android.booking.ui.webView.Booking this.webView.getSettings().setJavaScriptEnabled(true)
m com.liveperson.infra.messaging_ui.fragment.CobrowseF webView.getSettings().setJavaScriptEnabled(true);
m cartrawler.core.ui.modules.payment.options.paypal.Pz settings.setJavaScriptEnabled(true);
m com.united.mobile.android.homescreen.ui.qualtricsfee webSettings.setJavaScriptEnabled(true);
m com.liveperson.infra.messaging_ui.fragment.SecuredFc this.mWebView.getSettings().setJavaScriptEnabled(true)

```

Several locations where the setting is on. Most notably from google services + ads. Also some references to a variety of games such as a flight sim, a Santa sleigh game and a trivia game.

MASVS-PLATFORM-3:

Finding Sensitive Information in Auto-Generated Screenshots:

```

c androidx.media.AudioAttributesCompat static final int FLAG_SECURE = 2;

```

No Overlay Attacks found.

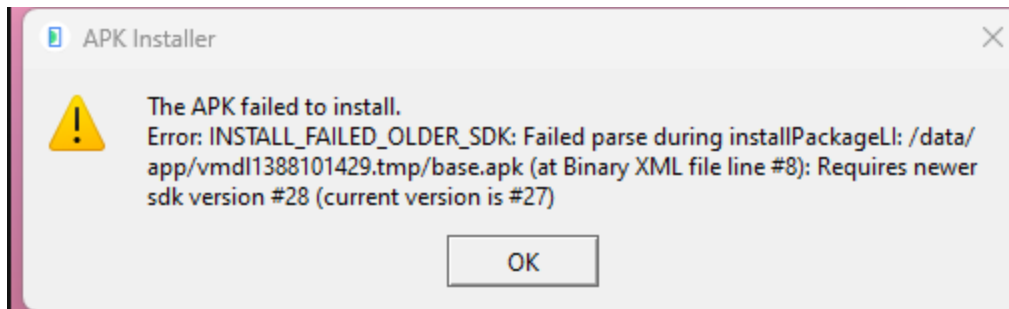
MASVS-CODE-1:

App has a minimum version of 28, below I tested the app on android api version 28

```

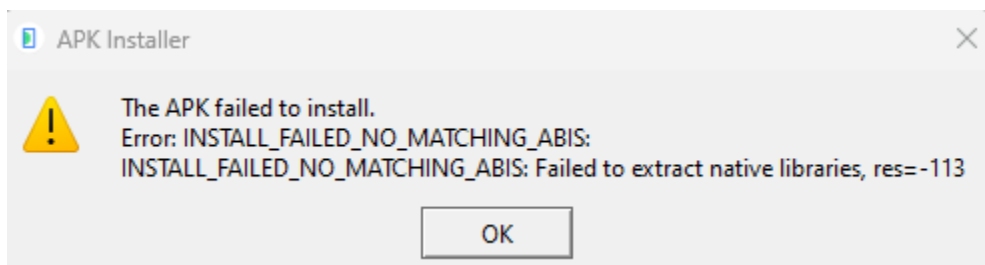
<manifest xmlns:android="http://schemas.android.com/apk/res/android" and
<uses-sdk android:minSdkVersion="28" android:targetSdkVersion="33"/>

```



MASVS-CODE-2:

I got an apk from APK Mirror for a united airlines version from 2017, when loading it into an api version 30 emulator it could not load:



I then Downloaded a versions from 2022 and app successfully installed and ran with no indications for enforced updates.

MASVS-CODE-3:

MobSF does not report vulnerable library's.

LIBRARIES

▼ Showing all 4 libraries

org.apache.http.legacy
android.ext.adservices
androidx.window.extensions
androidx.window.sidecar

MASVS-CODE-4:

EnableSafeBrowsing was not found

In testing the injection flaws on a rooted device, it seems that inputs are sanitized. In the following image testing on a rooted device the following error were received with the last command being of a export=false, used as a control to test the command's functionality:

```
Error while accessing provider:com.united.mobile.android.widget.tripCountDown.TripCountDownWidget
java.lang.IllegalStateException: Could not find provider: com.united.mobile.android.widget.tripC
dgetLargeProvider
    at com.android.commands.content.Content$Command.execute(Content.java:519)
    at com.android.commands.content.Content.main(Content.java:735)
    at com.android.internal.os.RuntimeInit.nativeFinishInit(Native Method)
    at com.android.internal.os.RuntimeInit.main(RuntimeInit.java:359)
emu64xa:/ # content query --uri content://androidx.biometric.DeviceCredentialHandlerActivity
Error while accessing provider:androidx.biometric.DeviceCredentialHandlerActivity
java.lang.IllegalStateException: Could not find provider: androidx.biometric.DeviceCredentialHan
    at com.android.commands.content.Content$Command.execute(Content.java:519)
    at com.android.commands.content.Content.main(Content.java:735)
    at com.android.internal.os.RuntimeInit.nativeFinishInit(Native Method)
    at com.android.internal.os.RuntimeInit.main(RuntimeInit.java:359)
content query --uri content://com.inmobile.MeshProvider
Error while accessing provider:com.inmobile.MeshProvider
java.lang.IllegalStateException: Could not find provider: com.inmobile.MeshProvider
    at com.android.commands.content.Content$Command.execute(Content.java:519)
    at com.android.commands.content.Content.main(Content.java:735)
    at com.android.internal.os.RuntimeInit.nativeFinishInit(Native Method)
    at com.android.internal.os.RuntimeInit.main(RuntimeInit.java:359)
content query --uri content://com.united.mobile.android.reservation.fileprovider
No result found.
```

```
    at com.android.internal.os.RuntimeInit.main(RuntimeInit.java:359)
content query --uri content://com.united.mobile.android.reservation.fileprovider --where "name='Bob') OR 1=1--'"
No result found.
content query --uri content://androidx.biometric.DeviceCredentialHandlerActivity --where "name='Bob') OR 1=1--'"
Error while accessing provider:androidx.biometric.DeviceCredentialHandlerActivity
java.lang.IllegalStateException: Could not find provider: androidx.biometric.DeviceCredentialHandlerActivity
    at com.android.commands.content.Content$Command.execute(Content.java:519)
    at com.android.commands.content.Content.main(Content.java:735)
    at com.android.internal.os.RuntimeInit.nativeFinishInit(Native Method)
    at com.android.internal.os.RuntimeInit.main(RuntimeInit.java:359)
roidx.biometric.DeviceCredentialHandlerActivity --where "name='Bob') OR 1=1--'"
Error while accessing provider:androidx.biometric.DeviceCredentialHandlerActivity
java.lang.IllegalStateException: Could not find provider: androidx.biometric.DeviceCredentialHandlerActivity
    at com.android.commands.content.Content$Command.execute(Content.java:519)
    at com.android.commands.content.Content.main(Content.java:735)
    at com.android.internal.os.RuntimeInit.nativeFinishInit(Native Method)
    at com.android.internal.os.RuntimeInit.main(RuntimeInit.java:359)
```

```
127|emu64xa:/ # whoami
root
emu64xa:/ #
```