



ANDROID STATIC ANALYSIS REPORT



 Albert Heijn (8.23.3)

File Name: com.icemobile.albertheijn_8.23.3-1806703336_minAPI21(arm64-v8a)(nodpi)_apkmirror.com.apk

Package Name: com.icemobile.albertheijn

Scan Date: Aug. 23, 2022, 2:08 p.m.






App Security Score: **35/100 (HIGH RISK)**

Grade:



Trackers Detection: 7/428

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
12	17	3	2	2

FILE INFORMATION

File Name: com.icemobile.albertheijn_8.23.3-1806703336_minAPI21(arm64-v8a)(nodpi)_apkmirror.com.apk

Size: 74.81MB

MD5: 97dfecb19394644c9e4b7a6606e3f19e

SHA1: e8ff81cd0fd3344409ec95b101946778af2cc151

SHA256: 0ceb2d0b02226b8c0a65ae7e9f9125b9e16cd11db111b5cc50923eba6bc9ea9b

APP INFORMATION

App Name: Albert Heijn

Package Name: com.icemobile.albertheijn

Main Activity:

Target SDK: 32

Min SDK: 21

Max SDK:

Android Version Name: 8.23.3

Android Version Code: 1806703336

APP COMPONENTS

Activities: 74

Services: 25

Receivers: 21

Providers: 7

Exported Activities: 5

Exported Services: 1

Exported Receivers: 7

Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed

v1 signature: True

v2 signature: True

v3 signature: False

Found 1 unique certificates

Subject: L=Amsterdam, O=IceMobile

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2010-05-21 10:26:06+00:00

Valid To: 2110-04-27 10:26:06+00:00

Issuer: L=Amsterdam, O=IceMobile

Serial Number: 0x4bf65fbe

Hash Algorithm: sha1

md5: 9e8959aa2756c9609aef61a2f25e1ab7

sha1: a1a4145da9a16941d74c8438bab6ef006124aa19

sha256: 8635e5cd6e4e61bf18446d3ca78e25c115b35ad9916c2b6f87e8a8be7a82891c

sha512: 9d9a41f77ebecfe272ee3cd2deac0c0c782ded244c8743a61436c972e3ddfd896c2ca5cfc128c1d51fabb930cd1c5ad739462ad97bcdce8b7a4742ab24cd10b1

PublicKey Algorithm: rsa

Bit Size: 1024

Fingerprint: e84d211c1fb2de59aece48022bcab7cb2798c0f352e0dbfe93bf07ea69481bf5

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

Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.android.alarm.permission.SET_ALARM	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

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.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.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
com.google.android.gms.permission.AD_ID	unknown	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.POST_NOTIFICATIONS	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	signature	C2DM	Permission for cloud to device messaging.

		permissions	
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
com.icemobile.albertheijn.batch.permission.INTERNAL_BROADCAST	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check subscriber ID check ro.kernel.qemu check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8
classes2.dex	FINDINGS	DETAILS

	Compiler	r8 without marker (suspicious)
classes3.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)
classes4.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.MANUFACTURER check
	Compiler	r8 without marker (suspicious)
lib/arm64-v8a/libstdc-core.so	FINDINGS	DETAILS
	Anti-VM Code	possible VM check

BROWSABLE ACTIVITIES

--	--

ACTIVITY	INTENT
nl.ah.appie.app.splash.DeepLinkActivity	Schemes: http://, https://, appie://, Hosts: ah.nl, www.ah.nl, tst.ah.nl, acc.ah.nl, ah.be, www.ah.be, tst.ah.be, acc.ah.be, nieuwsbrief.ah.nl, albertheijn.onelink.me, Path Patterns: /ahmiles, /ahtogo, /allerhande, /allerhande/favorieten, /allerhande/recept/R-R.*, /allerhande/zoeken/wat-heb-je-nog-in-huis, /appactie/*.*, /bonus, /bonus/folder/*.*, /bonus/volgende-week, /bonusbox, /checkin, /digitaalsparen, /digitaalsparen/*.*, /digitaalsparen/overmaken/*.*, /koopzegels, /mb, /mijn-ah-bonuskaart, /mijnbestellingen, /mijnlijst, /mijnreserveringen, /mr, /my-ah-promotion, /one-time-change-address, /producten, /producten/, /producten/eerder-gekocht/bestellingen, /producten/eerder-gekocht?.*\$, /producten/product/volgende-week/wi.*, /producten/product/wi.*, /producten/*.*, /profiel, /r/*.*, /smartwalkingroute.*, /thema/*.*, /winkels, /zoeken.*,
nl.ah.appie.debitcardtokenization.presentation.enroll.DebitCardTokenizationEnrollmentActivity	Schemes: http://, https://, Hosts: ah.nl, www.ah.nl, tst.ah.nl, acc.ah.nl, ah.be, www.ah.be, tst.ah.be, acc.ah.be, Path Patterns: /debit-card-tokenization/enroll.*,
com.adyen.threeds2.internal.ui.activity.ChallengeActivity	Schemes: adyen3ds2://, Hosts: com.icemobile.albertheijn,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
1	clients1.google.com	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Activity-Alias (com.icemobile.albertheijn.ui.activity.SplashActivity) is not Protected. [android:exported=true]	high	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.
3	Activity (nl.ah.appie.app.splash.DeepLinkActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Broadcast Receiver (com.appsflyer.MultipleInstallBroadcastReceiver) is not Protected. [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Broadcast Receiver (com.google.android.gms.analytics.CampaignTrackingReceiver) is not Protected. [android:exported=true]	high	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.
6	Activity (nl.ah.appie.debitcardtokenization.presentation.enroll.DebitCardTokenizationEnrollmentActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
			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

7	<p>Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]</p>	warning	<p>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.</p>
8	<p>Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]</p>	warning	<p>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.</p>
9	<p>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]</p>	warning	<p>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.</p>
10	<p>Activity (com.adyen.threeds2.internal.ui.activity.ChallengeActivity) is not Protected. [android:exported=true]</p>	high	<p>An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the</p>

			device.
11	Broadcast Receiver (com.adyen.threeds2.internal.AppUpgradeBroadcastReceiver) is not Protected. [android:exported=true]	high	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.
12	Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Broadcast Receiver (com.batch.android.BatchPushMessageReceiver) 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.
14	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ee/a.java oc/za1.java oc/z2.java oc/v7.java ec/a0.java cg/j0.java m8/b0.java ux/g.java bc/t.java oc/yf2.java bf/c.java ef/p.java cc/f.java h3/c.java oc/bh.java com/philips/codedlightcommon/CameraKt.j ava v3/g.java z8/q.java ob/a.java h3/d.java oc/j0.java cg/q.java sa/d.java oc/lf.java jc/m.java ff/g.java ef/b0.java oc/ea0.java com/appsflyer/internal/u.java d8/l.java ob/f1.java bc/e.java oc/ve2.java zk/h.java

wc/q5.java
oc/q.java
io/flutter/plugin/editing/b.java
n3/j.java
x2/f.java
x9/c.java
xf/d.java
oc/hd.java
s4/n.java
oc/vk2.java
m8/l.java
com/philips/indoormaps/logic/TiledView.java
ch/a.java
cg/a0.java
cc/i.java
com/philips/codedlightcommon/CodedLightLogger.java
com/baseflow/geolocator/a.java
el/c.java
com/batch/android/g0/q.java
bd/q0.java
h3/w.java
fc/v0.java
t8/l.java
f4/a.java
t8/b0.java
cg/e.java
f00/a.java
oc/zj2.java
h3/h.java
ef/l.java
ag/c.java
cf/c.java
ed/a.java
io/flutter/embedding/engine/a.java
com/batch/android/f/r.java
ef/s.java
wc/n2.java
oc/kl2.java
com/journeyapps/barcodescanner/b.java
cl/e.java

n4/q.java
bc/l.java
com/philips/codedlightcommon/Camera.java
t8/c.java
com/bumptechnology/gl意思ide/c.java
w3/b.java
ok/a.java
com/philips/indoorpositioning/library/IPBluetooth.java
t8/d.java
cg/c0.java
ai/l.java
c8/b.java
d3/c.java
oc/cp1.java
oc/h0.java
ec/t0.java
oc/fo2.java
oc/c4.java
a7/e.java
oc/qb2.java
ec/d.java
com/bumptechnology/gl意思ide/load/data/b.java
l6/b.java
fl/q.java
oc/dc0.java
com/batch/android/i0/b.java
fd/g0.java
oc/e7.java
com/bumptechnology/gl意思ide/GeneratedAppGlideModuleImpl.java
oc/zt.java
k5/a.java
ef/m0.java
oc/zc.java
oc/n1.java
oc/f2.java
jf/e.java
k3/j.java
j3/h.java
bc/c.java

oc/oc2.java
t8/j.java
u4/b.java
cg/l0.java
qc/f.java
s6/b.java
ob/l.java
oc/o0.java
cg/b0.java
com/appsflyer/internal/y.java
nk/a.java
oc/n6.java
zh/k.java
oc/fm2.java
ob/u.java
ff/b.java
fd/s7.java
g/b.java
fc/r0.java
s4/p.java
k3/h.java
k3/k.java
ai/j.java
h3/o.java
io/flutter/plugin/platform/b.java
com/bumptechnology/h.java
ec/r0.java
d5/c.java
oc/kp1.java
q8/r.java
cg/t0.java
o4/e0.java
wc/p5.java
lf/b.java
k3/g.java
cg/m0.java
s4/b0.java
com/batch/android/d0/f.java
d4/a.java
ef/k.java
i2/r.java
ux/f.java

n8/j.java
iq0/d.java
c3/d.java
w7/i.java
com/appsflyer/internal/ba.java
oc/t0.java
jc/d.java
oc/xb.java
s3/b.java
cg/j.java
z8/s.java
x8/i.java
cg/v0.java
oc/vh2.java
nl/ah/appie/app/tabs/TabActivity.java
oc/qc.java
mk/c.java
ld/g.java
h60/b.java
ef/y.java
zp0/b.java
bc/g.java
ef/o.java
wc/e5.java
com/philips/indoorpositioning/library/IPLoc
ation.java
mk/h.java
fl/d.java
io/flutter/embedding/android/a.java
jc/l.java
p6/k.java
cc/e.java
qk/d.java
oc/g2.java
ai/g.java
oc/yf.java
cg/w.java
c5/q.java
com/journeyapps/barcodescanner/a.java
g/m.java
mk/j.java
oc/h1.java

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

ce/d.java
he/b.java
cg/q0.java
fd/d7.java
oc/fg.java
v3/i.java
oc/hr1.java
h3/r.java
cg/g.java
oc/mn0.java
k3/o.java
wc/n1.java
ok/c.java
oc/cn2.java
b5/a.java
com/appsflyer/AFLogger.java
oc/dp0.java
p0/c1.java
mk/k.java
wc/o0.java
wb/s.java
com/appsflyer/internal/ab.java
p001if/a.java
oc/zi2.java
cc/b0.java
io/flutter/plugin/editing/d.java
d2/k.java
bc/o.java
mk/g.java
j8/e.java
oc/au0.java
oc/x7.java
com/appsflyer/internal/bu.java
m/f.java
com/batch/android/j0/c.java
lb/b.java
x8/a.java
com/appsflyer/internal/by.java
l3/a.java
l3/e.java
oc/m4.java
com/appsflyer/internal/i.java

cb/q.java
io/flutter/embedding/android/c.java
oc/x9.java
fc/b.java
fc/d1.java
fj0/h.java
fc/c1.java
h/i.java
oc/pc.java
je/e.java
fd/b.java
x4/b.java
b7/k.java
cg/y.java
fc/k0.java
af/e.java
com/appsflyer/internal/bs.java
cg/o.java
zf/b.java
oc/ba.java
com/batch/android/e/b.java
io/flutter/view/AccessibilityViewEmbedder.j
ava
oc/w9.java
ef/k0.java
m8/i.java
oc/h7.java
cc/s.java
w4/c.java
ff/e.java
nc/b.java
za/a.java
ef/f0.java
com/bumptechnology/load/resource/bitmap
/DefaultImageHeaderParser.java
fc/x.java
oc/xb2.java
mc/i.java
hq0/h.java
id/a.java
fc/f.java
s4/y.java

cc/w.java
bc/r.java
ef/x.java
oc/k2.java
oc/bg.java
lf/e.java
zk/a.java
d9/d.java
cc/h.java
u2/d.java
s3/a0.java
j3/f.java
u3/d.java
j8/d.java
c5/m0.java
oc/v1.java
com/batch/android/f0.java
ux/e.java
ef/m.java
nl/ah/appie/profile/bonuscard/BonusCard
OnboardingActivity.java
wc/q0.java
wc/m5.java
s3/a.java
bc/b.java
ze/j.java
ai/f.java
g8/c.java
q8/e.java
k3/i.java
c5/v0.java
ai/b.java
f8/j.java
oc/r2.java
d8/n.java
com/journeyapps/barcodescanner/Capture
Activity.java
wc/r5.java
h/q.java
com/bumptech/glide/i.java
va/k.java
oc/xa.java

bf/e.java
o8/e.java
cg/p0.java
s3/c0.java
yk/c.java
wc/k5.java
com/batch/android/MessagingActivity.java
com/bumptechnology/load/data/l.java
com/bumptechnology/load/data/j.java
ef/z.java
f4/b.java
t8/m.java
h/t.java
com/baseflow/geolocator/GeolocatorLocationService.java
qc/h.java
c5/h.java
oc/zf2.java
com/philips/indoormaplogic/MapFragment.java
io/flutter/plugins/GeneratedPluginRegistrant.java
s3/l0.java
oc/r3.java
fd/x2.java
d9/j.java
cg/k0.java
com/bumptechnology/load/engine/GlideException.java
ob/k0.java
oc/tc.java
ad/e.java
bh/e.java
oc/a2.java
f8/g.java
m5/k.java
el/a.java
p8/a.java
n8/i.java
oc/r6.java
lf/d.java
kf/d.java

a7/b.java
af/c.java
com/batch/android/d0/c.java
zk/d.java
oc/wp1.java
ve/d.java
oc/ab.java
ob/i.java
com/batch/android/g0/b.java
p6/m.java
oc/hm2.java
n3/e.java
com/batch/android/d0/h.java
lb/a.java
t8/z.java
ic/a.java
l8/a.java
io/flutter/plugin/platform/j.java
fc/a0.java
ge/d.java
v3/c.java
q8/c.java
je/g.java
m8/n.java
c9/k.java
io/flutter/plugin/platform/SingleViewPresent
ation.java
z3/c.java
oc/se2.java
d7/b.java
h9/a.java
yk/k.java
df/c.java
bh/d.java
oc/bl2.java
z8/m.java
com/batch/android/j0/b.java
s8/a.java
oc/x.java
oc/y41.java
cg/m.java
oc/mw1.java

				t8/q.java oc/ig2.java ff/h.java z8/n.java oc/hi2.java oc/pa2.java io/flutter/embedding/engine/FlutterJNI.java d3/a.java bf/d.java s3/l.java ef/q.java ef/e.java h/p.java c1/e.java m4/i.java com/batch/android/e/a.java oc/Cif.java ef/h0.java jf/f.java bc/q.java o8/j.java oc/s12.java ke/c.java ai/a.java d4/b.java ec/c0.java com/philips/indoorpositioning/library/IPCo nnection.java ef/c0.java uc/u.java p6/a.java
2	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	oc/ar.java oc/xi.java atd/n/a.java cb/q.java oc/jq.java i3/b.java cl/b.java
	App creates temp file. Sensitive		CWE: CWE-276: Incorrect Default Permissions	jp/espresso3389/pdf_render/a.java

3	information should never be written into a temp file.	warning	OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	cg/q.java zf/d.java s4/b0.java
4	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/batch/android/c1/f.java sa/c.java fd/l.java com/batch/android/q/d.java oc/j51.java com/batch/android/q/c.java cb/f0.java oc/r51.java com/batch/android/s/c.java fd/d7.java com/batch/android/b1/a.java q9/e.java oc/z41.java fd/b.java fd/r2.java cb/a0.java cb/h0.java cb/c0.java iz/a.java q9/c.java fd/m.java ab/a.java com/batch/android/s/b.java cb/d0.java cb/e0.java fd/r7.java x4/a.java cb/g0.java com/batch/android/c1/b.java
				p9/a.java oc/kc2.java wc/n2.java oc/ki2.java oc/qb2.java oc/dc0.java oc/e7.java

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	yh/b.java oc/in.java am/b.java atd/r0/g.java j\$/util/concurrent/ThreadLocalRandom.java com/appsflyer/internal/b.java fd/k7.java am/a.java wb/h.java c5/o0.java bm/a.java com/batch/android/f/o0.java nj0/j.java f8/j.java q4/e.java z8/b.java nl/ah/appie/stamps/presentation/ui/Stamp CardView.java
6	Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	dw/a.java
7	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	oc/ad0.java com/batch/android/g0/e.java fa0/e.java
				com/batch/android/Batch.java nl/ah/appie/listlogic/mylist/persistence/v2/ CommonListLineDataV2.java defpackage/nd.java b80/c.java nl/ah/appie/dto/smartwalkingroute/License .java nl/ah/appie/dto/purchasestamps/Secret.jav a oc/g.java com/adyen/checkout/components/model/p

8	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	ayments/request/CardPaymentMethod.java a m8/r.java com/adyen/checkout/adyen3ds2/model/FingerprintToken.java com/batch/android/BatchActionActivity.java a p0/y0.java nl/ah/appie/dto/member/MemberUnsubscribeRequest.java nl/ah/appie/listlogic/mylist/persistence/v1/ListLineDataV1.java com/batch/android/BatchMessage.java com/batch/android/BatchPushJobService.java
9	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	xo/b0.java an0/g.java c20/k.java an0/b.java
10	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	gr0/e.java rq0/a.java qq0/a.java tq0/c.java pq0/a.java sq0/a.java
11	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	oc/in.java com/batch/android/f/n.java fd/k7.java com/appsflyer/internal/ai.java oc/mh.java oc/t6.java oc/m80.java
12	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography	fm0/a.java oc/m7.java

	oracle attacks.		OWASP MASVS: MSTG-CRYPTO-3	
13	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	aj/a.java cg/w.java com/appsflyer/internal/ai.java com/batch/android/f/a.java zf/b.java ef/e.java
14	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	io/flutter/plugin/editing/a.java yk/h.java com/batch/android/b/a.java com/batch/android/i/a.java
15	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	j9/x.java c5/m0.java w9/a.java ef/e.java
16	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	l9/b.java hq0/c.java hq0/d.java zi/c2.java zi/w1.java hq0/h.java hq0/g.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
		True info The shared object has NX bit set. This marks a	True info This shared object has a stack canary value	None info The shared	None info The shared object does	True info The shared object has the following fortified	True info Symbols are stripped.

1	lib/arm64-v8a/libsdcbbarcode.so	memory page non-executable making attacker injected shellcode non-executable.	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.	object does not have run-time search path or RPATH set.	not have RUNPATH set.	functions: ['__memcpy_chk', '__memmove_chk']	
2	lib/arm64-v8a/libsdccore.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__memcpy_chk', '__vsprintf_chk', '__strlen_chk', '__strchr_chk', '__memmove_chk']	True info Symbols are stripped.
3	lib/arm64-v8a/libbbhelper.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.

4	lib/arm64-v8a/libindoorpositioning.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>True info</p> <p>The shared object has the following fortified functions: ['_vsnprintf_chk', '_strlen_chk', '_vsprintf_chk', '_strncat_chk', '_strcat_chk', '_strncpy_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>
5	lib/arm64-v8a/libmapprootkit.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>True info</p> <p>The shared object has the following fortified functions: ['_strlen_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>
6	lib/arm64-v8a/libscanditsdk-android-6.13.1.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>True info</p> <p>The shared object has the following fortified functions: ['_strchr_chk', '_memmove_chk', '_strlen_chk', '_vsnprintf_chk', '_read_chk', '_memcpy_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

			verifying the integrity of the canary before function return.	set.			
7	lib/arm64-v8a/libapp.so	False high The shared object does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.	False high This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
8	lib/arm64-v8a/libflutter.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['_vsprintf_chk', '_read_chk', '_memcpy_chk', '_strlen_chk', '_strcpy_chk', '_strncpy_chk', '_memmove_chk']	True info Symbols are stripped.
		True info The shared object has NX bit set. This marks a memory page non-executable making	True info This shared object has a stack canary value added to the stack so that it will be	None info The shared object does not	None info The shared object does not have RUNPATH	True info The shared object has the following fortified functions: ['_memmove_chk',	True info Symbols are stripped.

9	lib/arm64-v8a/libbar.so	attacker injected shellcode non-executable.	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.	have run-time search path or RPATH set.	set.	'__strlen_chk', '__vsprintf_chk', '__read_chk']	
---	-------------------------	---	--	---	------	---	--

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['location', 'camera', 'network connectivity', 'bluetooth'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.

8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower.
12	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode or AES-GCM (as defined in NIST SP 800-38D) and cryptographic key sizes 256-bit/128-bit.
13	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
14	FCS_COP.1.1(4)	Selection-Based Security Functional Requirements	Cryptographic Operation - Keyed-Hash Message Authentication	The application perform keyed-hash message authentication with cryptographic algorithm ['HMAC-SHA-256'] .
15	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
16	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional	HTTPS Protocol	The application implement HTTPS using TLS.

		Requirements		
17	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
18	FIA_X509_EXT.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The application validate the revocation status of the certificate using the Online Certificate Status Protocol (OCSP) as specified in RFC 2560 or a Certificate Revocation List (CRL) as specified in RFC 5759 or an OCSP TLS Status Request Extension (i.e., OCSP stapling) as specified in RFC 6066', 'The certificate path must terminate with a trusted CA certificate'].
19	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
20	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.
21	FCS_CKM.1.1(2)	Optional Security Functional Requirements	Cryptographic Symmetric Key Generation	The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
cdn-testsettings.appsflyersdk.com	ok	IP: 0.0.0.0 Country: - Region: - City: - Latitude: 0.000000

		Longitude: 0.000000 View: Google Map
www.example.com	ok	IP: 93.184.216.34 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
clients1.google.com	ok	IP: 172.217.4.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
support.google.com	ok	IP: 142.250.191.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
checkoutshopper-live.adyen.com	ok	IP: 147.12.16.90 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
qr.ah	ok	No Geolocation information available.
		IP: 0.0.0.0 Country: -

cdn-settings.appsflyersdk.com	ok	Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
sgcdsdk.s	ok	No Geolocation information available.
sars.s	ok	No Geolocation information available.
wa.me	ok	IP: 157.240.249.60 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
sadrevenue.s	ok	No Geolocation information available.
checkoutshopper-live-au.adyen.com	ok	IP: 85.184.231.70 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
goo.gl	ok	IP: 142.250.191.238 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
		IP: 0.0.0.0 Country: - Region: -

googleads.g.doubleclick.net	ok	City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
www.ah.be	ok	IP: 23.56.168.73 Country: United States of America Region: Illinois City: Chicago Latitude: 41.850029 Longitude: -87.650047 View: Google Map
bf51022iye.bf.dynatrace.com	ok	IP: 108.129.14.8 Country: Ireland Region: Dublin City: Dublin Latitude: 53.343990 Longitude: -6.267190 View: Google Map
app-measurement.com	ok	IP: 0.0.0.0 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
mijnahmiles.ah.nl	ok	IP: 87.233.198.83 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
		IP: 172.217.4.78 Country: United States of America Region: California

google.com	ok	City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
checkoutshopper-test.adyen.com	ok	IP: 147.12.17.151 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
sstats.s	ok	No Geolocation information available.
firebase.google.com	ok	IP: 172.217.1.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
simpresion.s	ok	No Geolocation information available.
api.whatsapp.com	ok	IP: 157.240.2.53 Country: United States of America Region: Illinois City: Chicago Latitude: 41.850029 Longitude: -87.650047 View: Google Map
staging.sdk-api.scandit.com	ok	IP: 54.77.14.25 Country: Ireland Region: Dublin City: Dublin Latitude: 53.343990 Longitude: -6.267190

		View: Google Map
github.com	ok	IP: 140.82.114.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
wsmetrics.batch.com	ok	IP: 0.0.0.0 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
twitter.com	ok	IP: 104.244.42.129 Country: United States of America Region: California City: San Francisco Latitude: 37.773968 Longitude: -122.410446 View: Google Map
ahold.com	ok	IP: 40.118.81.46 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
staging-imagecollection.scandit.com	ok	IP: 3.69.178.232 Country: Germany Region: Hessen City: Frankfurt am Main Latitude: 50.115520 Longitude: 8.684170

		View: Google Map
slaunches.s	ok	No Geolocation information available.
sattr.s	ok	No Geolocation information available.
bf83228gpx.bf.dynatrace.com	ok	IP: 52.215.34.144 Country: Ireland Region: Dublin City: Dublin Latitude: 53.343990 Longitude: -6.267190 View: Google Map
pagead2.google syndication.com	ok	IP: 0.0.0.0 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
plus.google.com	ok	IP: 172.217.1.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
ws.batch.com	ok	IP: 0.0.0.0 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
sonelink.s	ok	No Geolocation information available.

forms.office.com	ok	IP: 13.107.6.194 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
www.ing.nl	ok	IP: 23.66.167.251 Country: United States of America Region: Illinois City: Mount Prospect Latitude: 42.066422 Longitude: -87.937286 View: Google Map
zsp2.ah.nl	ok	IP: 13.249.141.86 Country: United States of America Region: Illinois City: Chicago Latitude: 41.850029 Longitude: -87.650047 View: Google Map
ns.adobe.com	ok	No Geolocation information available.
www.airmiles.nl	ok	IP: 20.86.233.73 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
static.ah.nl	ok	IP: 104.88.206.9 Country: United States of America Region: Massachusetts City: Cambridge

		Latitude: 42.363598 Longitude: -71.085205 View: Google Map
www.ah.nl	ok	IP: 23.56.168.9 Country: United States of America Region: Illinois City: Chicago Latitude: 41.850029 Longitude: -87.650047 View: Google Map
checkoutshopper-live-us.adyen.com	ok	IP: 135.84.148.134 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
www.googleadservices.com	ok	IP: 0.0.0.0 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
developers.google.com	ok	IP: 142.250.191.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
sdlsdk.s	ok	No Geolocation information available.
		IP: 13.249.141.60 Country: United States of America

journeyapps.com	ok	Region: Illinois City: Chicago Latitude: 41.850029 Longitude: -87.650047 View: Google Map
exoplayer.dev	ok	IP: 185.199.110.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map
imasdk.googleapis.com	ok	IP: 172.217.1.106 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
play.google.com	ok	IP: 142.250.191.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
sapp.s	ok	No Geolocation information available.
sinapps.s	ok	No Geolocation information available.
selfscan.store.ah.nl	ok	IP: 172.16.8.3 Country: - Region: - City: - Latitude: 0.000000

		Longitude: 0.000000 View: Google Map
svalidate.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
www.kpn.com	ok	IP: 54.230.18.76 Country: United States of America Region: Illinois City: Chicago Latitude: 41.850029 Longitude: -87.650047 View: Google Map
www.google.com	ok	IP: 142.250.191.132 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
goo.gle	ok	IP: 67.199.248.12 Country: United States of America Region: New York City: New York City Latitude: 40.739288 Longitude: -73.984955 View: Google Map
www.2s	ok	No Geolocation information available.
m.me	ok	IP: 157.240.2.20 Country: United States of America Region: Illinois City: Chicago Latitude: 41.850029 Longitude: -87.650047

		View: Google Map
ah.nl	ok	IP: 23.56.168.19 Country: United States of America Region: Illinois City: Chicago Latitude: 41.850029 Longitude: -87.650047 View: Google Map
sconversions.s	ok	No Geolocation information available.
csi.gstatic.com	ok	IP: 0.0.0.0 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
api.ah.nl	ok	IP: 23.56.168.67 Country: United States of America Region: Illinois City: Chicago Latitude: 41.850029 Longitude: -87.650047 View: Google Map
admob-gmats.uc.r.appspot.com	ok	IP: 142.250.191.116 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
mjolnir.mopinion.com	ok	IP: 0.0.0.0 Country: - Region: - City: -

		Latitude: 0.000000 Longitude: 0.000000 View: Google Map
www.efteling.com	ok	IP: 13.226.22.70 Country: United States of America Region: Illinois City: Chicago Latitude: 41.850029 Longitude: -87.650047 View: Google Map
misc.hotspotsvankpn.com	ok	IP: 82.94.177.183 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
schemas.android.com	ok	No Geolocation information available.
ah-online-ga-bigquery.firebaseio.com	ok	IP: 34.120.160.131 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
sregister.s	ok	No Geolocation information available.
imagecollection.scandit.com	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.
www.w3.org	ok	No Geolocation information available.

drws.batch.com	ok	No Geolocation information available.
developer.android.com	ok	No Geolocation information available.
sdk-api.scandit.com	ok	No Geolocation information available.
bankieren.rabobank.nl	ok	No Geolocation information available.
batch.com	ok	No Geolocation information available.
issuetracker.google.com	ok	No Geolocation information available.
googlemobileadssdk.page.link	ok	No Geolocation information available.

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://ah-online-ga-bigquery.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
this@listfragment.lifecycle	ya0/z.java
u0013android@android.com0 u0013android@android.com	cc/r.java

testpanel@ahold.nl bla@bla.com	Android String Resource
appro@openssl.org	lib/arm64-v8a/libflutter.so

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Batch	Analytics, Profiling	https://reports.exodus-privacy.eu.org/trackers/23
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Scandit	Analytics	https://reports.exodus-privacy.eu.org/trackers/84

HARDCODED SECRETS

POSSIBLE SECRETS
"com_batchsdk_local_campaign_debug_fragment_token" : "Token"
"connected_card_authorized_close" : "Sluiten"

"connected_card_authorized_title" : "Gelukt!"
"firebase_database_url" : "https://ah-online-ga-bigquery.firebaseio.com"
"firebase_sender_id" : "951744672057"
"google_api_key" : "AlzaSyBx1GJDZxV-LPLqnARkm4aOdaldNEoNdBI"
"google_crash_reporting_api_key" : "AlzaSyBx1GJDZxV-LPLqnARkm4aOdaldNEoNdBI"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"login_view_show_password" : "Toon"

Report Generated by - MobSF v3.5.2 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.

© 2022 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).