ANDROID STATIC ANALYSIS REPORT

Aptoide (9.17.3.0)

File Name:	smartplug.apk
Package Name:	cm.aptoide.pt
Scan Date:	June 13, 2024, 7:34 a.m.
App Security Score:	22/100 (CRITICAL RISK)
Grade:	F
Trackers Detection:	16/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
50	29	2	3	4

FILE INFORMATION

File Name: smartplug.apk
Size: 19.74MB
MD5: 54670c9735d27cc4b7dd97c765351ac6
SHA1: 956b674706063c93b4f5e88ee6a943a185ba5774
SHA256: 829f8ca5b4efe9b1c542aed86ebeeef7b4912c73bd5c0456b371dad6280c7882

APP INFORMATION

App Name: Aptoide
Package Name: cm.aptoide.pt
Main Activity: cm.aptoide.pt.view.MainActivity
Target SDK: 25
Min SDK: 16
Max SDK:
Android Version Name: 9.17.3.0

Android Version Code: 10040

APP COMPONENTS

Activities: 37
Services: 13
Receivers: 19
Providers: 6
Exported Activities: 2
Exported Services: 4
Exported Receivers: 6
Exported Providers: 1

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: ST=Portugal
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2009-09-22 14:53:51+00:00
Valid To: 2034-09-16 14:53:51+00:00
Issuer: ST=Portugal
Serial Number: 0x4ab8e4ff
Hash Algorithm: sha1
md5: 99bd1872bc56b4b2619e731ae9cbdc6f
sha1: d590a7d792fd0331542d99faf9997641790773a9
sha256: 73534d45c1345a4783c7eff2cf6038551ab5fdf09673f32c68c3b0864baa80e4
sha512: 8a5562a7825800df284d47dab79fcae1ccde0c3c46b1a181696809ed270576b92718130131ffef402f4d2822e235879de1e91224d91f0f4c0a0b58d2d2bc5b43
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.READ_SYNC_STATS	normal	read sync statistics	Allows an application to read the sync stats; e.g. the history of syncs that have occurred.
com.android.launcher.permission.INSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
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.INSTALL_PACKAGES	SignatureOrSystem	directly install applications	Allows an application to install new or updated Android packages. Malicious applications can use this to add new applications with arbitrarily powerful permissions.
android.permission.CHANGE_WIFI_MULTICAST_STATE	normal	allow Wi-Fi Multicast reception	Allows an application to receive packets not directly addressed to your device. This can be useful when discovering services offered nearby. It uses more power than the non-multicast mode.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_SYNC_SETTINGS	normal	read sync settings	Allows an application to read the sync settings, such as whether sync is enabled for Contacts.
android.permission.WRITE_SYNC_SETTINGS	normal	write sync settings	Allows an application to modify the sync settings, such as whether sync is enabled for Contacts.
android.permission.AUTHENTICATE_ACCOUNTS	dangerous	act as an account authenticator	Allows an application to use the account authenticator capabilities of the Account Manager, including creating accounts as well as obtaining and setting their passwords.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible Build.SERIAL check
network operator name check
device ID check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
SIM operator check
network operator name check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.BOARD check
Build.TAGS check
SIM operator check
network operator name check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.cm.aptoide.pt,

ACTIVITY	INTENT
cm.aptoide.pt.DeepLinkIntentReceiver	Schemes: file://, http://, aptoide://, aptoiderepo://, aptoidexml://, aptoideinstall://, aptoideauth://, aptoidesearch://, aptword://, aptoidefeature://, market://, https://, Hosts: app.aptoide.com, market.android.com, webservices.aptoide.com, play.google.com, imgs.aptoide.com, *.en.aptoide.com, *.pt.aptoide.com, *.br.aptoide.com, *.fr.aptoide.com, *.es.aptoide.com, *.mx.aptoide.com, *.de.aptoide.com, *.it.aptoide.com, *.ru.aptoide.com, *.sa.aptoide.com, *.id.aptoide.com, *.in.aptoide.com, *.bd.aptoide.com, *.mr.aptoide.com, *.pa.aptoide.com, *.my.aptoide.com, *.th.aptoide.com, *.vn.aptoide.com, *.tr.aptoide.com, *.cn.aptoide.com, *.ro.aptoide.com, *.mm.aptoide.com, *.pl.aptoide.com, *.rs.aptoide.com, *.hu.aptoide.com, *.gr.aptoide.com, *.bg.aptoide.com, *.nl.aptoide.com, *.ir.aptoide.com, en.aptoide.com, pt.aptoide.com, br.aptoide.com, fr.aptoide.com, es.aptoide.com, mx.aptoide.com, de.aptoide.com, it.aptoide.com, ru.aptoide.com, sa.aptoide.com, id.aptoide.com, in.aptoide.com, bd.aptoide.com, mr.aptoide.com, pa.aptoide.com, my.aptoide.com, th.aptoide.com, vn.aptoide.com, tr.aptoide.com, cn.aptoide.com, ro.aptoide.com, mm.aptoide.com, pl.aptoide.com, rs.aptoide.com, hu.aptoide.com, gr.aptoide.com, bg.aptoide.com, nl.aptoide.com, ir.aptoide.com, community.aptoide.com, Mime Types: application/vnd.cm.aptoide.pt, Path Prefixes: /apkinstall, Path Patterns: *//.myapp, /store/..*, /thank-you*, /using-appcoins*, /download*, /editorial/..*, /app, /,

NETWORK SECURITY

HIGH: **0** | WARNING: **1** | INFO: **1** | SECURE: **0**

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	info	Base config is configured to trustbundled certs @raw/vanilla_cert.
2	*	warning	Base config is configured to trust system certificates.

CERTIFICATE ANALYSIS

HIGH: **2** | WARNING: **0** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	high	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 vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 44 | WARNING: 17 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.1-4.1.2, [minSdk=16]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Launch Mode of activity (cm.aptoide.pt.view.MainActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
4	Activity (cm.aptoide.pt.view.MainActivity) is vulnerable to Android Task Hijacking/StrandHogg.	high	An Activity should not be having the launch mode attribute set to "singleTask". It is then possible for other applications to place a malicious activity on top of the activity stack resulting in Task Hijacking/StrandHogg 1.0 vulnerability. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" or by setting an empty taskAffinity (taskAffinity="") attribute. You can also update the target SDK version (25) of the app to 28 or higher to fix this issue at platform level.
5	TaskAffinity is set for activity (cm.aptoide.pt.wallet.WalletInstallActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
6	Service (cm.aptoide.pt.account.AccountAuthenticatorService) is not Protected. An intent-filter exists.	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Content Provider (cm.aptoide.pt.toolbox.ToolboxContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity (com.facebook.CustomTabActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (25) of the app to 29 or higher to fix this issue at platform level.
9	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://app.aptoide.com]	high	App Link asset verification URL (http://app.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
11	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=https://app.aptoide.com]	high	App Link asset verification URL (https://app.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
12	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://market.android.com]	high	App Link asset verification URL (http://market.android.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
13	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://webservices.aptoide.com]	high	App Link asset verification URL (http://webservices.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
14	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=https://webservices.aptoide.com]	high	App Link asset verification URL (https://webservices.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: None). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
15	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://play.google.com]	high	App Link asset verification URL (http://play.google.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
16	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://imgs.aptoide.com]	high	App Link asset verification URL (http://imgs.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
17	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=https://imgs.aptoide.com]	high	App Link asset verification URL (https://imgs.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
18	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://en.aptoide.com]	high	App Link asset verification URL (http://en.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
19	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://pt.aptoide.com]	high	App Link asset verification URL (http://pt.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
20	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://br.aptoide.com]	high	App Link asset verification URL (http://br.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
21	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://fr.aptoide.com]	high	App Link asset verification URL (http://fr.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
22	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://es.aptoide.com]	high	App Link asset verification URL (http://es.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
23	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://mx.aptoide.com]	high	App Link asset verification URL (http://mx.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
24	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=https://mx.aptoide.com]	high	App Link asset verification URL (https://mx.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
25	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://de.aptoide.com]	high	App Link asset verification URL (http://de.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
26	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://it.aptoide.com]	high	App Link asset verification URL (http://it.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
27	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://ru.aptoide.com]	high	App Link asset verification URL (http://ru.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
28	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://sa.aptoide.com]	high	App Link asset verification URL (http://sa.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
29	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://id.aptoide.com]	high	App Link asset verification URL (http://id.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
30	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://in.aptoide.com]	high	App Link asset verification URL (http://in.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
31	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://bd.aptoide.com]	high	App Link asset verification URL (http://bd.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
32	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://mr.aptoide.com]	high	App Link asset verification URL (http://mr.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
33	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://pa.aptoide.com]	high	App Link asset verification URL (http://pa.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
34	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://my.aptoide.com]	high	App Link asset verification URL (http://my.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
35	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://th.aptoide.com]	high	App Link asset verification URL (http://th.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
36	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://vn.aptoide.com]	high	App Link asset verification URL (http://vn.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
37	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://tr.aptoide.com]	high	App Link asset verification URL (http://tr.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
38	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://cn.aptoide.com]	high	App Link asset verification URL (http://cn.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
39	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://ro.aptoide.com]	high	App Link asset verification URL (http://ro.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
40	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://mm.aptoide.com]	high	App Link asset verification URL (http://mm.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
41	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://pl.aptoide.com]	high	App Link asset verification URL (http://pl.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
42	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://rs.aptoide.com]	high	App Link asset verification URL (http://rs.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
43	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://hu.aptoide.com]	high	App Link asset verification URL (http://hu.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
44	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://gr.aptoide.com]	high	App Link asset verification URL (http://gr.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
45	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://bg.aptoide.com]	high	App Link asset verification URL (http://bg.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
46	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://nl.aptoide.com]	high	App Link asset verification URL (http://nl.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
47	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://ir.aptoide.com]	high	App Link asset verification URL (http://ir.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
48	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://community.aptoide.com]	high	App Link asset verification URL (http://community.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
49	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=https://community.aptoide.com]	high	App Link asset verification URL (https://community.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
50	TaskAffinity is set for activity (cm.aptoide.pt.DeepLinkIntentReceiver)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
51	Activity (cm.aptoide.pt.DeepLinkIntentReceiver) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (25) of the app to 29 or higher to fix this issue at platform level.

NO	ISSUE	SEVERITY	DESCRIPTION
52	Activity (cm.aptoide.pt.DeepLinkIntentReceiver) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
53	Broadcast Receiver (cm.aptoide.pt.install.InstalledBroadcastReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
54	Broadcast Receiver (cm.aptoide.pt.notification.NotificationReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
55	Broadcast Receiver (cm.aptoide.pt.install.CheckRootOnBoot) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
56	Broadcast Receiver (cm.aptoide.pt.widget.SearchWidgetProvider) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
57	Broadcast Receiver (com.vungle.warren.NetworkStateReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
58	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
59	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
60	Service (com.appnext.base.services.OperationJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
61	Broadcast Receiver (com.appnext.base.receivers.AppnextBootReciever) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
62	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

CODE ANALYSIS

HIGH: **3** | WARNING: **10** | INFO: **1** | SECURE: **3** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				cm/aptoide/aptoideviews/common/StringUtilsKt.java cm/aptoide/aptoideviews/downloadprogressview/DownloadProgressView$stateMachine$1.java cm/aptoide/pt/app/view/AppCoinsInfoFragment.java cm/aptoide/pt/crashreports/CrashReport.java cm/aptoide/pt/editorial/EditorialFragment.java cm/aptoide/pt/editorialList/EditorialListFragment.java cm/aptoide/pt/home/HomeFragment.java cm/aptoide/pt/install/installer/Root.java cm/aptoide/pt/install/remote/RemoteInstallationSenderManager.java cm/aptoide/pt/logger/Logger.java cm/aptoide/pt/networking/image/ImageLoa

NO	ISSUE	SEVERITY	STANDARDS	FILES
				cm/aptoide/pt/networking/image/ImageLoader.java cm/aptoide/pt/notification/NotificationWorker.java cm/aptoide/pt/root/RootShell.java cm/aptoide/pt/root/containers/RootClass.java cm/aptoide/pt/toolbox/ToolboxContentProvider.java com/airbnb/epoxy/i.java com/airbnb/epoxy/p.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/c.java com/airbnb/lottie/d.java com/airbnb/lottie/e.java com/airbnb/lottie/f.java com/airbnb/lottie/l.java com/airbnb/lottie/r/a.java com/airbnb/lottie/r/b.java com/airbnb/lottie/u/c.java com/airbnb/lottie/u/g.java com/airbnb/lottie/u/u.java com/applovin/adview/b.java com/applovin/adview/e.java com/appnext/ads/interstitial/InterstitialActivity.java com/appnext/appnextsdk/API/AppnextAdRequest.java com/appnext/base/operations/imp/cdm.java com/appnext/base/operations/imp/sals.java com/appnext/base/services/logic/AlarmServiceLogic.java com/appnext/base/utils/SdkHelper.java com/appnext/core/AppnextHelperClass.java com/appnext/sdk/adapters/mopub/ads/AppnextMoPubCustomEvent.java com/appnext/sdk/adapters/mopub/ads/AppnextMoPubCustomEventFullScreenVideo.java com/appnext/sdk/adapters/mopub/ads/App

NO	ISSUE	SEVERITY	STANDARDS	FILES
				nextMoPubCustomEventInterstitial.java com/appnext/sdk/adapters/mopub/ads/AppnextMoPubCustomEventRewardedVideo.java com/appnext/sdk/adapters/mopub/ads/AppnextMoPubRewardedVideo.java com/appnext/sdk/adapters/mopub/ads/Helper.java com/appnext/sdk/adapters/mopub/banners/AppnextMoPubCustomEventBanner.java com/appnext/sdk/adapters/mopub/nativeads/AppnextMoPubCustomNativeAd.java com/appnext/sdk/adapters/mopub/nativeads/native_ads2/AppnextMoPubCustomEventNative.java com/appnext/sdk/adapters/mopub/nativeads/native_ads2/AppnextMoPubCustomNativeAd.java com/asf/appcoins/sdk/core/util/LogInterceptor.java com/bumptech/glide/c.java com/bumptech/glide/l/d.java com/bumptech/glide/l/e.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/a0/e.java com/bumptech/glide/load/engine/a0/i.java com/bumptech/glide/load/engine/b0/a.java com/bumptech/glide/load/engine/b0/b.java com/bumptech/glide/load/engine/h.java com/bumptech/glide/load/engine/i.java com/bumptech/glide/load/engine/k.java com/bumptech/glide/load/engine/y.java com/bumptech/glide/load/engine/z/j.java com/bumptech/glide/load/engine/z/k.java com/bumptech/glide/load/m/b.java com/bumptech/glide/load/m/j.java com/bumptech/glide/load/m/l.java com/bumptech/glide/load/m/o/c.java com/bumptech/glide/load/m/o/e.java com/bumptech/glide/load/n/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/n/d.java com/bumptech/glide/load/n/f.java com/bumptech/glide/load/n/s.java com/bumptech/glide/load/n/t.java com/bumptech/glide/load/o/c/c.java com/bumptech/glide/load/o/c/j.java com/bumptech/glide/load/o/c/l.java com/bumptech/glide/load/o/c/m.java com/bumptech/glide/load/o/c/q.java com/bumptech/glide/load/o/c/w.java com/bumptech/glide/load/o/c/y.java com/bumptech/glide/load/o/g/a.java com/bumptech/glide/load/o/g/d.java com/bumptech/glide/load/o/g/j.java com/bumptech/glide/m/e.java com/bumptech/glide/m/f.java com/bumptech/glide/m/k.java com/bumptech/glide/m/l.java com/bumptech/glide/m/n.java com/bumptech/glide/m/o.java com/bumptech/glide/n/d.java com/bumptech/glide/p/j.java com/bumptech/glide/p/l/j.java com/bumptech/glide/q/a.java com/bumptech/glide/r/l/a.java com/flurry/sdk/a.java com/fyber/inneractive/sdk/a/a.java com/fyber/inneractive/sdk/activities/InneractiveInternalBrowserActivity.java com/fyber/inneractive/sdk/config/IAConfigManager.java com/fyber/inneractive/sdk/external/InneractiveAdViewUnitController.java com/fyber/inneractive/sdk/f/d.java com/fyber/inneractive/sdk/f/h.java com/fyber/inneractive/sdk/f/j.java com/fyber/inneractive/sdk/i/d.java com/fyber/inneractive/sdk/j/b/a/g.java com/fyber/inneractive/sdk/l/a.java com/fyber/inneractive/sdk/util/IAlog.java com/fyber/inneractive/sdk/util/u.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/inmobi/commons/core/utilities/Logger.java com/integralads/avid/library/inmobi/utils/AvidLogs.java com/integralads/avid/library/mopub/utils/AvidLogs.java com/moat/analytics/mobile/inm/m.java com/moat/analytics/mobile/inm/p.java com/moat/analytics/mobile/sma/m.java com/moat/analytics/mobile/sma/p.java com/moat/analytics/mobile/vng/m.java com/moat/analytics/mobile/vng/p.java com/mopub/common/MoPub.java com/mopub/common/logging/MoPubDefaultLogger.java com/mopub/common/privacy/MoPubIdentifier.java com/mopub/mobileads/AppLovinBanner.java com/mopub/mobileads/AppLovinInterstitial.java com/mopub/mobileads/AppLovinRewardedVideo.java com/mopub/mobileads/MoPubActivity.java com/mopub/mobileads/MraidActivity.java com/mopub/mobileads/RewardedMraidActivity.java com/mopub/mraid/MraidController.java com/mopub/nativeads/InMobiBannerCustomEvent.java com/mopub/nativeads/InMobiInterstitialCustomEvent.java com/mopub/nativeads/InMobiNativeCustomEvent.java com/mopub/nativeads/InMobiRewardedCustomEvent.java com/mopub/nativeads/InneractiveBannerCustomEvent.java com/mopub/nativeads/InneractiveInterstitialCustomEvent.java com/mopub/network/MultiAdResponse.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	com/mopub/volley/CacheDispatcher.java com/mopub/volley/NetworkDispatcher.java com/mopub/volley/VolleyLog.java com/mopub/volley/toolbox/BasicNetwork.java com/mopub/volley/toolbox/DiskBasedCache.java com/mopub/volley/toolbox/HttpHeaderParser.java com/mopub/volley/toolbox/ImageRequest.java com/mopub/volley/toolbox/JsonRequest.java com/smaato/soma/g0/b.java com/smaato/soma/h0/k/b.java com/smaato/soma/j0/r.java com/smaato/soma/j0/s.java com/smaato/soma/j0/t.java com/smaato/soma/j0/u.java com/smaato/soma/l0/a.java com/unity3d/ads/metadata/InAppPurchaseMetaData.java com/unity3d/ads/metadata/MetaData.java com/unity3d/services/UnityServices.java com/unity3d/services/ads/UnityAdsImplementation.java com/unity3d/services/ads/adunit/AdUnitActivity.java com/unity3d/services/ads/adunit/VideoPlayerHandler.java com/unity3d/services/ads/api/AdUnit.java com/unity3d/services/ads/api/VideoPlayer.java com/unity3d/services/ads/api/WebPlayer.java com/unity3d/services/ads/configuration/AdsModuleConfiguration.java com/unity3d/services/ads/video/VideoPlayerView.java com/unity3d/services/ads/webplayer/WebPlayer.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/unity3d/services/ar/ARUtils.java com/unity3d/services/ar/view/ARView.java com/unity3d/services/ar/view/GLSurfaceView.java com/unity3d/services/ar/view/ShaderLoader.java com/unity3d/services/banners/UnityBanners.java com/unity3d/services/banners/api/Banner.java com/unity3d/services/banners/view/BannerView.java com/unity3d/services/core/api/Cache.java com/unity3d/services/core/api/DeviceInfo.java com/unity3d/services/core/api/Intent.java com/unity3d/services/core/api/Request.java com/unity3d/services/core/api/Sdk.java com/unity3d/services/core/broadcast/BroadcastEventReceiver.java com/unity3d/services/core/cache/CacheDirectory.java com/unity3d/services/core/cache/CacheThread.java com/unity3d/services/core/cache/CacheThreadHandler.java com/unity3d/services/core/configuration/Configuration.java com/unity3d/services/core/configuration/EnvironmentCheck.java com/unity3d/services/core/configuration/InitializeThread.java com/unity3d/services/core/connectivity/ConnectivityMonitor.java com/unity3d/services/core/device/AdvertisingId.java com/unity3d/services/core/device/Device.java com/unity3d/services/core/device/Storage.java com/unity3d/services/core/log/DeviceLog.ja

NO	ISSUE	SEVERITY	STANDARDS	FILES
				va com/unity3d/services/core/misc/JsonStorage.java com/unity3d/services/core/misc/Utilities.java com/unity3d/services/core/misc/ViewUtilities.java com/unity3d/services/core/preferences/AndroidPreferences.java com/unity3d/services/core/properties/ClientProperties.java com/unity3d/services/core/properties/SdkProperties.java com/unity3d/services/core/request/WebRequest.java com/unity3d/services/core/request/WebRequestRunnable.java com/unity3d/services/core/request/WebRequestThread.java com/unity3d/services/core/sensorinfo/SensorInfoListener.java com/unity3d/services/core/webview/WebView.java com/unity3d/services/core/webview/WebViewApp.java com/unity3d/services/core/webview/bridge/Invocation.java com/unity3d/services/core/webview/bridge/NativeCallback.java com/unity3d/services/core/webview/bridge/WebViewBridge.java com/unity3d/services/core/webview/bridge/WebViewBridgeInterface.java com/unity3d/services/core/webview/bridge/WebViewCallback.java com/unity3d/services/monetization/UnityMonetization.java com/unity3d/services/monetization/core/utilities/JSONUtilities.java com/unity3d/services/monetization/placementcontent/core/PlacementContent.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/unity3d/services/purchasing/core/TransactionDetailsUtilities.java com/unity3d/services/purchasing/core/TransactionErrorDetailsUtilities.java com/unity3d/services/purchasing/core/api/CustomPurchasing.java com/vungle/warren/AdvertisementPresenterFactory.java com/vungle/warren/Storage.java com/vungle/warren/Vungle.java com/vungle/warren/VungleJobRunner.java com/vungle/warren/download/APKDirectDownloadManager.java com/vungle/warren/model/Advertisement.java com/vungle/warren/model/Cookie.java com/vungle/warren/model/Placement.java com/vungle/warren/model/Report.java com/vungle/warren/network/APKDirectDownloader.java com/vungle/warren/network/FetchDownloader.java com/vungle/warren/network/VungleApiClient.java com/vungle/warren/persistence/FilePersistor.java com/vungle/warren/persistence/GraphicDesigner.java com/vungle/warren/presenter/LocalAdPresenter.java com/vungle/warren/presenter/WebAdPresenter.java com/vungle/warren/tasks/CleanupJob.java com/vungle/warren/tasks/DownloadJob.java com/vungle/warren/tasks/JobInfo.java com/vungle/warren/tasks/SendReportsJob.java com/vungle/warren/tasks/runnable/JobRunnable.java com/vungle/warren/ui/JavascriptBridge.java com/vungle/warren/ui/VungleActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/vungle/warren/ui/VungleFlexViewActivity.java com/vungle/warren/ui/VungleNativeView.java com/vungle/warren/ui/VungleWebClient.java com/vungle/warren/ui/VungleWebViewActivity.java com/vungle/warren/utility/FileUtility.java i/a/k/a/a.java i/a/o/g.java i/h/e/b.java i/h/e/d.java i/h/e/e.java i/h/e/f.java i/h/e/i.java i/h/e/j.java i/h/j/b.java i/h/k/b.java i/h/l/b.java i/h/l/d0/c.java i/h/l/e.java i/h/l/g.java i/h/l/u.java i/h/l/v.java i/h/l/x.java i/j/a/c.java i/l/a/b.java i/l/b/c.java i/m/a/a.java i/n/a.java i/n/b.java i/o/a/b.java i/q/a/c.java i/r/a/c.java i/s/i0.java i/s/y.java i/t/a/i.java io/rakam/api/i.java k/b/a/a/a.java k/c/a/b/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				k/c/a/b/d.java k/c/a/b/d0.java k/c/a/c/c.java k/c/a/c/c0.java k/c/a/c/p6.java k/c/a/c/t5.java k/c/d/o.java k/c/d/p.java k/g/b/b/m/h.java k/g/b/b/w/d.java k/g/b/b/x/b.java k/g/b/b/z/g.java n/b/g/a.java n/b/g/b.java n/b/g/d/a/a.java q/c/g/j.java
				cm/aptoide/pt/BuildConfig.java cm/aptoide/pt/DeepLinkIntentReceiver.java cm/aptoide/pt/account/AccountAnalytics.java cm/aptoide/pt/account/AndroidAccountManagerPersistence.java cm/aptoide/pt/account/view/LoginSignUpCredentialsFragment.java cm/aptoide/pt/app/view/MoreBundleFragment.java cm/aptoide/pt/bottomNavigation/BottomNavigationActivity.java cm/aptoide/pt/database/room/RoomNotification.java cm/aptoide/pt/database/room/RoomStore.java cm/aptoide/pt/dataprovider/WebService.java cm/aptoide/pt/dataprovider/model/v3/CheckUserCredentialsJson.java cm/aptoide/pt/home/HomeFragment.java cm/aptoide/pt/home/bundles/BundlesRepository.java cm/aptoide/pt/networking/Pnp1Authorizatio

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	nInterceptor.java cm/aptoide/pt/preferences/LocalPersistenceAdultContent.java cm/aptoide/pt/preferences/managed/ManagedKeys.java cm/aptoide/pt/promotions/ClaimPromotionDialogFragment.java cm/aptoide/pt/themes/ThemeManager.java cm/aptoide/pt/util/PreferencesXmlParser.java cm/aptoide/pt/view/DeepLinkManager.java cm/aptoide/pt/view/app/ListStoreAppsFragment.java cm/aptoide/pt/view/fragment/GridRecyclerSwipeWithToolbarFragment.java cm/aptoide/pt/view/settings/SettingsFragment.java com/appnext/base/database/repo/ConfigDataRepo.java com/appnext/base/database/repo/DataRepo.java com/appnext/base/utils/ConfigDataUtils.java com/appnext/base/utils/Constants.java com/appnext/base/utils/LibrarySettings.java com/appnext/base/utils/SdkHelper.java com/appnext/sdk/adapters/mopub/ads/AppnextMoPubCustomEvent.java com/appnext/sdk/adapters/mopub/banners/AppnextMoPubCustomEventBanner.java com/appnext/sdk/adapters/mopub/banners/Helper.java com/appnext/sdk/adapters/mopub/nativeads/AppnextMoPubCustomEventNative.java com/appnext/sdk/adapters/mopub/nativeads/native_ads2/AppnextMoPubCustomEventNative.java com/bumptech/glide/load/engine/d.java com/bumptech/glide/load/engine/p.java com/bumptech/glide/load/engine/w.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/h.java com/mopub/common/Constants.java com/mopub/common/DataKeys.java com/mopub/common/GpsHelper.java com/mopub/common/MoPubBrowser.java com/mopub/mobileads/BaseVideoPlayerActivity.java com/unity3d/ads/metadata/InAppPurchaseMetaData.java com/vungle/warren/tasks/DownloadJob.java k/c/a/c/h1.java n/b/l/g/k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	cm/aptoide/pt/BuildConfig.java com/appnext/ads/fullscreen/FullscreenAdsManager.java com/appnext/ads/fullscreen/Video.java com/appnext/ads/interstitial/Interstitial.java com/appnext/ads/interstitial/InterstitialActivity.java com/appnext/appnextsdk/API/Native.java com/appnext/appnextsdk/API/NativeAdObject.java com/appnext/banners/BannerAd.java com/appnext/banners/JSBannerAdapter.java com/appnext/core/AdsManager.java com/appnext/core/AppnextHelperClass.java com/appnext/core/BuildConfig.java com/appnext/nativeads/NativeAd.java com/appnext/nativeads/NativeAdObject.java com/fyber/inneractive/sdk/g/a/l.java com/fyber/inneractive/sdk/video/IAVideoKit.java com/mopub/mobileads/UnityAdsAdapterConfiguration.java com/mopub/mobileads/admob/BuildConfig.java com/mopub/mobileads/vungle/BuildConfig.java com/mopub/nativeads/AppnextBaseAdapterConfiguration.java com/mopub/nativeads/InMobiBaseAdapterConfiguration.java o/a/g/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	cm/aptoide/pt/ApplicationModule.java cm/aptoide/pt/abtesting/ABTestServiceProvider.java cm/aptoide/pt/dataprovider/WebService.java com/aptoide/authentication/network/RemoteAuthenticationService.java com/asf/appcoins/sdk/contractproxy/AppCoinsAddressProxyBuilder.java com/flurry/sdk/n1.java com/inmobi/ads/bh.java com/vungle/warren/network/VungleApiClient.java
5	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	cm/aptoide/pt/ApplicationModule.java cm/aptoide/pt/AptoideApplication.java cm/aptoide/pt/install/installer/DefaultInstaller.java cm/aptoide/pt/view/ActivityModule.java com/flurry/sdk/k4.java com/fyber/inneractive/sdk/external/InneractiveAdManager.java com/fyber/inneractive/sdk/g/a/l.java com/fyber/inneractive/sdk/l/d.java com/fyber/inneractive/sdk/util/i.java com/mopub/mraid/MraidNativeCommandHandler.java com/unity3d/services/core/cache/CacheDirectory.java com/vungle/warren/download/APKDirectDownloadManager.java com/vungle/warren/network/VungleApiClient.java k/c/a/c/h0.java n/b/g/d/a/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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/appnext/base/database/DatabaseSqlHelper.java com/inmobi/commons/core/d/b.java com/liulishuo/filedownloader/services/b.java com/liulishuo/filedownloader/services/c.java i/q/a/g/a.java io/rakam/api/b.java k/k/a/a.java
7	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	cm/aptoide/pt/download/FileDownloadTask.java cm/aptoide/pt/utils/AptoideUtils.java com/appnext/core/AppnextHelperClass.java com/fyber/inneractive/sdk/g/a/e.java k/i/a/f0/f.java
8	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	cm/aptoide/pt/preferences/PRNGFixes.java cm/aptoide/pt/utils/AptoideUtils.java com/flurry/sdk/j.java com/fyber/inneractive/sdk/g/a/e.java com/inmobi/commons/core/utilities/a/b.java com/mopub/common/util/Utils.java com/smaato/soma/h0/k/c.java com/unity3d/services/core/device/Device.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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	cm/aptoide/pt/ads/AdsRepository.java cm/aptoide/pt/utils/AptoideUtils.java com/appnext/ads/TemplateRandomizer.java com/appnext/ads/fullscreen/FullscreenActivity.java com/appnext/ads/fullscreen/Video.java com/appnext/appnextsdk/API/AppnextAPI.java com/appnext/banners/TemplateRandomizer.java com/appnext/base/services/logic/ServiceSchedulingLogic.java com/appnext/core/AdsManager.java com/appnext/core/AppnextHelperClass.java com/appnext/sdk/adapters/mopub/nativeads/AppnextMoPubCustomNativeAd.java com/inmobi/ads/cache/a.java com/inmobi/commons/core/network/c.java com/inmobi/rendering/a/a.java io/sentry/connection/l.java k/c/a/a/n.java o/a/g/h.java o/a/g/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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	com/appnext/banners/JSBannerAdapter.java com/appnext/core/result/ResultPageActivity.java com/appnext/core/webview/AppnextWebView.java com/inmobi/rendering/RenderView.java com/smaato/soma/f0/a.java com/unity3d/services/ads/webplayer/WebPlayer.java com/unity3d/services/core/webview/WebView.java com/vungle/warren/ui/VungleActivity.java com/vungle/warren/ui/VungleNativeView.java
11	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	cm/aptoide/pt/account/view/PhotoFileGenerator.java i/n/b.java
12	Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system.	warning	CWE: CWE-200: Information Exposure OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/unity3d/services/core/webview/WebView.java com/vungle/warren/ui/VungleWebViewActivity.java
13	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/fyber/inneractive/sdk/l/a.java k/c/a/b/g.java
14	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/appnext/base/utils/Generator.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
15	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. 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	com/mopub/network/CustomSSLSocketFactory.java
16	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	n/b/g/d/a/a.java
17	This App uses SafetyNet API.	secure	OWASP MASVS: MSTG-RESILIENCE-7	cm/aptoide/pt/analytics/FirstLaunchAnalytics.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/24	android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_WIFI_STATE, android.permission.GET_ACCOUNTS, android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	3/45	com.android.launcher.permission.INSTALL_SHORTCUT, android.permission.AUTHENTICATE_ACCOUNTS, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

TYPE	MATCHES	PERMISSIONS

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION
config.inmobi.cn	IP: 39.105.228.126 Country: China Region: Zhejiang City: Hangzhou
i.l.inmobicdn.cn	IP: 42.177.83.115 Country: China Region: Liaoning City: Shenyang

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
api.appnxt.net	ok	No Geolocation information available.
github.com	ok	**IP:** 20.205.243.166 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
dock.inmobi.com	ok	No Geolocation information available.
crash-metrics.sdk.inmobi.com	ok	**IP:** 172.212.5.164 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.731323 **Longitude:** -73.990089 **View:** Google Map
i.l.inmobicdn.net	ok	**IP:** 152.199.39.108 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.034081 **Longitude:** -77.488503 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
diagnostics.rakam.io	ok	**IP:** 172.67.215.225 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sdkm.w.inmobi.com	ok	**IP:** 172.212.5.164 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.731323 **Longitude:** -73.990089 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
cdn.appnext.com	ok	**IP:** 108.157.14.18 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.aptoide.com	ok	**IP:** 34.251.203.24 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
developer.android.com	ok	**IP:** 172.217.24.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
apis.appnxt.net	ok	No Geolocation information available.
d.applvn.com	ok	**IP:** 104.17.1.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
global.appnext.com	ok	**IP:** 52.221.124.115 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cw50.smaato.net	ok	**IP:** 3.84.66.209 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
data.flurry.com	ok	**IP:** 106.10.248.146 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
vungle.com	ok	**IP:** 141.193.213.11 **Country:** United States of America **Region:** Texas **City:** Austin **Latitude:** 30.271158 **Longitude:** -97.741699 **View:** Google Map
www.aptoide.com	ok	**IP:** 52.18.176.43 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.mopub.com	ok	**IP:** 34.111.170.5 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
rt.applovin.com	ok	**IP:** 34.117.147.68 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
a.applovin.com	ok	**IP:** 34.117.147.68 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.facebook.com	ok	**IP:** 163.70.158.35 **Country:** France **Region:** Ile-de-France **City:** Nanterre **Latitude:** 48.891979 **Longitude:** 2.206750 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sdk-android.ad.smaato.net	ok	**IP:** 13.214.220.79 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
play.google.com	ok	**IP:** 142.251.220.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
apichain-dev.blockchainds.com	ok	No Geolocation information available.
www.amazon.com	ok	**IP:** 108.157.16.203 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.example.com	ok	**IP:** 93.184.215.14 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.vungle.com	ok	**IP:** 44.207.210.41 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
mobile-static.adsafeprotected.com	ok	**IP:** 18.65.25.31 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
telemetry.sdk.inmobi.com	ok	**IP:** 20.39.59.149 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **View:** Google Map
pool.img.aptoide.com	ok	**IP:** 172.67.29.206 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	**IP:** 195.15.222.169 **Country:** Switzerland **Region:** Basel-Stadt **City:** Basel **Latitude:** 47.558399 **Longitude:** 7.573270 **View:** Google Map
schemas.applovin.com	ok	No Geolocation information available.
twitter.com	ok	**IP:** 104.244.42.65 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
i.w.inmobi.com	ok	**IP:** 20.247.188.88 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
m.google.com	ok	**IP:** 142.251.220.75 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
vid.applovin.com	ok	**IP:** 34.160.64.118 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
rt.applvn.com	ok	**IP:** 104.17.2.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.inmobi.com	ok	**IP:** 20.81.69.107 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
d.applovin.com	ok	**IP:** 34.110.179.88 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
config.inmobi.com	ok	**IP:** 20.39.59.188 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **View:** Google Map
config.inmobi.cn	ok	**IP:** 39.105.228.126 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
sentry.aptoide.com	ok	**IP:** 34.243.65.15 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
api.blockchainds.com	ok	**IP:** 52.208.243.187 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cdn6.aptoide.com	ok	**IP:** 104.22.10.83 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
apichain.blockchainds.com	ok	**IP:** 18.202.192.78 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
a.applvn.com	ok	**IP:** 104.17.2.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
docs.sentry.io	ok	**IP:** 76.76.21.93 **Country:** United States of America **Region:** California **City:** Walnut **Latitude:** 34.015400 **Longitude:** -117.858223 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
webservices.aptoide.com	ok	**IP:** 37.48.77.165 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
m.aptoide.com	ok	**IP:** 37.48.77.161 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
admin.appnext.com	ok	**IP:** 18.205.15.225 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
z.moatads.com	ok	**IP:** 184.29.45.201 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ads.api.vungle.com	ok	**IP:** 3.233.247.27 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
imgs.aptoide.com	ok	**IP:** 37.48.77.161 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
config.unityads.unity3d.com	ok	**IP:** 34.110.229.214 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
cdn2.inner-active.mobi	ok	**IP:** 192.229.145.170 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sdktm.w.inmobi.com	ok	**IP:** 172.212.5.164 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.731323 **Longitude:** -73.990089 **View:** Google Map
catappult.io	ok	**IP:** 108.157.14.62 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
en.aptoide.com	ok	**IP:** 34.255.239.224 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
i.l.inmobicdn.cn	ok	**IP:** 42.177.83.115 **Country:** China **Region:** Liaoning **City:** Shenyang **Latitude:** 41.792221 **Longitude:** 123.432777 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
placeimg.com	ok	**IP:** 159.65.240.55 **Country:** United States of America **Region:** New Jersey **City:** Clifton **Latitude:** 40.858429 **Longitude:** -74.163757 **View:** Google Map
www.youtube.com	ok	**IP:** 142.250.71.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ws75-primary.aptoide.com	ok	**IP:** 37.48.77.180 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
a913.smaato.net	ok	**IP:** 52.0.242.118 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ws75.aptoide.com	ok	**IP:** 54.72.2.14 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
www.appnext.com	ok	**IP:** 18.234.79.235 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
blog.aptoide.com	ok	**IP:** 37.48.77.171 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
aptoi.de	ok	**IP:** 52.23.47.7 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

✉ EMAILS

EMAIL	FILE
485bb7b111d41f17e0f8@sentry.aptoide	cm/aptoide/pt/BuildConfig.java
support@aptoide.com	cm/aptoide/pt/AptoideApplication.java
filipo@emailo.como	com/aptoide/authentication/mock/MockAuthenticationService.java
creative-review@mopub.com	com/mopub/mobileads/AdAlertReporter.java
support@mopub.com	com/mopub/common/privacy/PersonalInfoManager.java
adqualitysupport@smaato.com	com/smaato/soma/h0/m/a.java
aptoide@aptoide.com support@aptoide.com suport@aptoide.com □□□suport@aptoide.com□□□□□□□	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AppLovin (MAX and SparkLabs)	Analytics, Profiling, Identification, Advertisement	https://reports.exodus-privacy.eu.org/trackers/72
Appnext		https://reports.exodus-privacy.eu.org/trackers/184

TRACKER	CATEGORIES	URL
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Flurry	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/25
Fyber	Advertisement	https://reports.exodus-privacy.eu.org/trackers/104
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Inmobi		https://reports.exodus-privacy.eu.org/trackers/106
Integral Ad Science		https://reports.exodus-privacy.eu.org/trackers/218
Moat	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/61
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447
Smaato		https://reports.exodus-privacy.eu.org/trackers/83
Twitter MoPub	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/35
Unity3d Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/121
Vungle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/169

HARDCODED SECRETS

POSSIBLE SECRETS
"password" : "Password"
"search_suggestion_provider_authority" : "cm.aptoide.pt.provider.SearchSuggestionProvider"
"store_suggestion_provider_authority" : "cm.aptoide.pt.provider.StoreSearchSuggestionProvider"
"store_username" : "Nickname"
"username" : "Email"
"password" : "گذرواژه"
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b>□□□□□□□□□□□□□□□□□□□□□□□"
"password" : "□□□□□□"
"recover_password" : "□□□□□□□□□□□□□□□"
"store_username" : "Nickname"
"username" : "E□□□"
"password" : "პაროლი"
"store_username" : "Nickname"
"username" : "ელ-ფოსტა"
"password" : "■■■■■■"

POSSIBLE SECRETS
"store_username" : "■■■■■"
"username" : "■■■■"
"password" : "Passwort"
"store_username" : "Nick"
"username" : "E-Mail"
"password" : "Парола"
"store_username" : "Прякор"
"username" : "Имейл"
"nothing_inserted_user" : "■■■■■■■■■■■■■■■■■■■■■■(■■■■■■■■)■■■■■■■■■■■■■■■■■■■■"
"password" : "■■■■■■■■"
"recover_password" : "■■■■■■■■■■■■■■■■■"
"social_timeline_users_private" : "%d■■■■■■■■■■■"
"store_username" : "■■■■■■"
"username" : "■■■■■"
"password" : "Salasana"

POSSIBLE SECRETS
"store_username" : "Nimimerkki"
"username" : "Sähköposti"
"password" : "■■■■■■■"
"store_username" : "Nickname"
"store_username" : "Nickname"
"username" : "Email"
"password" : "Пароль"
"store_username" : "Nickname"
"store_username" : "Ψευδώνυμο"
"username" : "Email"
"password" : "Wachtwoord"
"store_username" : "Weergavenaam"
"username" : "E-mail"
"password" : "Hasło"
"store_username" : "Nickname"

POSSIBLE SECRETS
"username" : "Email"
"password" : "[redacted]"
"store_username" : "Nickname"
"username" : "[redacted]"
"username" : "Email"
"password" : "Parolă"
"store_username" : "Pseudonim"
"username" : "E-mail"
"store_username" : "Pseudo"
"username" : "Email"
"password" : "[redacted]"
"username" : "[redacted]"
"password" : "Lozinka"
"store_username" : "Nadimak"
"username" : "E-pošta"

POSSIBLE SECRETS
"password" : "Şifre"
"username" : "E-posta"
"password" : "Contraseña"
"store_username" : "Apodo"
"username" : "E-mail"
"username" : "E-mel"
"password" : "Password"
"store_username" : "Nickname"
"password" : "Palavra-passe"
"store_username" : "Alcunha"
"username" : "E-mail"
"password" : "Jelszó"
"store_username" : "Nickname"
"username" : "E-mail"
"password" : "Пароль"

POSSIBLE SECRETS
"store_username" : "Никнейм"
"username" : "E-mail"
"password" : "■□□■■■■□■□■■■■■■■■"
"store_username" : "■■■■■□■■■■"
"username" : "■■■■■■■□"
"com_facebook_device_auth_instructions" : "□□□<b>facebook.com/device</b>□□□□□□□□□"
"nothing_inserted_user" : "□□□□□□□□□□□□□□□□□"
"password" : "□□"
"recover_password" : "□□□□"
"store_username" : "□□"
"username" : "□□□□"
"password" : "Palavra-passe"
"store_username" : "Apelido"
"username" : "E-mail"
"com_facebook_device_auth_instructions" : "□□<b>facebook.com/device</b&gt□□□□□□□□□□□□□□"

POSSIBLE SECRETS
"com_facebook_device_auth_instructions" : "□□<b>facebook.com/device</b&gt□□□□□□□□□□□□"
cAajgxHlj7GTSEIzIYIQxmEloOSoJq7VOaxWHfv72QM=
SgMhksOnpMJMBH1JH74BErFMAiPE78L9kUpiye6ezUkIKoc+RVuDLvEf36QK5tpM
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
DRYWi0TWx0xeQUvY98UNqkz37+DffrKoPBm+2dnlFUG6mCEAnCrfVx/sGMEehzhv
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
IlJxA/RzEPbEgRJQH0LQ8KVHKqG3NyhvdpUemJxyiMg=
B3EEABB8EE11C2BE770B684D95219ECB
31669e84ce5b48709ff5435d7b674844
4a80b049dc4441b4a5e0af3d3cc1a00e

POSSIBLE SECRETS
308205653082034ca00302010202044df76b53300d06092a864886f70d01010505003073310b30090603550406130270743110300e06035504081307556e6b6e6f776e310f300d060355040713064c6973626f6131153013060355040a130c4361697861204d61676963613110300e060355040b1307556e6b6e6f776e311830160603550403130f4475617274652053696c7665697261302017 0d3131303631343134303831395a180f32303933303830323134303831395a3073310b30090603550406130270743110300e06035504081307556e6b6e6f776e310f300d060355040713064c6973626f6131153013060355040a130c4361697861204d61676963613110300e060355040b1307556e6b6e6f776e311830160603550403130f4475617274652053696c766569726130820222300d06092a864886f70d01010105000382020f003082020a02820201026cfe7512fa0c40520971ee83e227208e072a1e1962a4fd0cd5c709e33dc45ce856e9ddc2b9a918394e96ec462d5fea2db81c443b9dbedd75a1031a1f1593b86eef83302f9ecdc0dfd227a3e11ccedb056e58c79b9177dbefba122a390dac88a90a317cb55a9171ab428b46c2e29b5d7fef2e823f5985b9c165a1edba7c82b4f8d5e3aa346996019cb8b7bcc768f5fdae15975add5e53c1fc022e4c99dababf3a80c5a09680ba4b8889cc4399940d92d11c289268d3f2671b98f871964f21c5870d9a1c72c8fbea65a637a06643f246e733fff37b7db4020fd2b6e7343fdbac2ddd20f8a48710d944d8f76432a3225f72c6a50c4e76247fb9256f294eeb9e24080ad28094fbfcfa6e4b5a85d652b1c5d967b39ee1272955a134a0ff1e89bb01f98d710204c72ca4c9dd44ecdd81358a8ef920fa371edd1bfc097c81678aa31b059b9218eba5c0ed2c209bd799a3ecab19e5e3b0e3d18029bf156b37e091969b4e5ae5024475b038b4d841e0e88580fd433154f606f1f7c14527f00509dd7448911e1ec44cb1e94f7dce59459e95438c4a245103d14fff047f97d14bf38f1802d84727b0f3aa98e02e8840892c629e303f76965e186de1d92263ec17e35aa224c33856d59095cf9195042ebfb5fd4703ef8add7ccf923640f266c22e432232f5c6b0873d99ebd509f9e66a77506eabef04ae1d9cf5edb40e13bc1cff39917da8b70203010001300d06092a864886f70d01010505000382020200069a29624d30983fdec4c4bf685f2f479214fda52e272a74ae8aee8bc7aae441ba79977cdd251cf5b21c56ee631dd1e17da28a2bd87d1190b4c1cc440140251e38af40aa694e6d3965c31b36ade9deccde0ca403639031f44f42e395b575a125cd210fd54e9ac760af1ed72c7b91f8f771074f6cafe0d28ab840510ee98a46eb84225be218ff6f90d036f47ec2e7dbfa067e9498cc633e5cab354ab86013b4d8047312643cdfbb6b3654dc26a87af0f4d83b2b0c6ad28d026483788daeda241c8e2631311e0e0d48c6f9284904cc4df114336c207e4c4f468f80f82f2d6917d8ec6b9e63fa2a0f126f668f8220667c92d26d55b5da7a4144b8693c0dec479a3c63b1d43eb96868eac1cb786e2f4b327bad553fc9ffe2dada3ab11bd6b1d7a623a92e821192b0dbcdabf0e4c361561bb5abb970d11e477050d56957fc8961106d2aaf1f209cbdde733a7a6e0577fd35d32f048e887b0e92c9415871e5b0d7458fe682256494b6c9443d04a076842d56374ee4c184a5c64a71c6818eafaa6dcbd66aae917907080d4895b7b0c941a4fae00be891666c0bdeb8b9331d0ff61d7ec2c26b80156aa64263e925dc9d84279bdb1e27e0403b57c14a1b2647a98c858ee20c92b967fb1eb963147fe390958e7c914fce69e1e2eb06139279b70a8eeabe99500ddf04223c3343e5c9b2722635856c65593aae9d2dbf3da704f79e8145f008e
3CA30A86d04e65E6E388922deCe3eBD0F100F5d0
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
686479766013060971498190079908139321726943530014330540939446345918554318339765539424505774633321719753296399637136332111386476861244038034037280889270700 5449
1b2ec33c1a5a485bb7b111d41f17e0f8
Bl3RSPeFXX48+A41tWFMGRj6+1eT4NHtkwATNUdtNkM=
gjATLq4PR4tBy0NKJBUs0hq7sitSgRlGcsdxPuImAoM=

POSSIBLE SECRETS
SVqWumuteCQHvVIaALrOZXuzVVVeS7f4FGxxu6V+es4=
1db8206f0da6aa81bbdd2d99a82d9e14
uUwZgwDOxcBXrQcntwu+kYFpkiVkOaezL0WYEZ3anJc=
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
UZJDjsNp1+4M5x9cbbdflB779y5YRBcV6Z6rBMLIrO4=
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
uhLcqjqmx4nAmM3qRNIgYeeALxilkZ+lc3aGgO+rkRY=
j+Yj7UMoEzr9M6nnqL4N+TgP7ihZaPMbtnYW3NPxsNU=
Rd5vBa3cRt13XnZUPrTszYMRTqEgpzuKs4niQNpf2R+gTE/2OPB9o8u+o5NCRvjI
1OoeMBy/0f4cuo3Q6fO79anCMG2ySlElR0298tBh7pCa++J4MQSzo8NUX4DLdHow
SJ3SRTdt7T2FQX1UH4DWlnlLfmao1u+KeMI8XtxEgmSHdfgiJRyy0Txw8FmQ+pQw
729d17030014409c93487eb8fc5c909f
Y/1pb58VeX4F8K6fayOs4meS93jwIQ+AMpk0KVFaduEwXDgWis9Z812p7+pIfyJn
65d359455ad84498ba83ad0a6aaa4af9

POSSIBLE SECRETS
3noVyuO3zFOuhvGfjg9nufIidaw0HmgQ5EVdw6MbLqs=
308203643082024ca0030201020204503fc625300d06092a864886f70d01010505003073310b30090603550406130270743110300e06035504081307556e6b6e6f776e310f300d060355040713064c6973626f6e31153013060355040a130c4361697861204d61676963613110300e060355040b13074170746f696465311830160603550403130f4475617274652053696c76656972613020170d3132303833303139353933335a180f32303934313031393139353933335a3073310b30090603550406130270743110300e06035504081307556e6b6e6f776e310f300d060355040713064c6973626f6e31153013060355040a130c4361697861204d61676963613110300e060355040b13074170746f696465311830160603550403130f4475617274652053696c766569726130820122300d06092a864886f70d01010105000382010f003082010a0282010100a7032cb40819b62cd596bc1c121951724e9a7d6612222d63dab58a18970339f77911b8e2a0665aa15efb051d4dd710c99e1fcaea006a651b7c113a71649c315e27122b9e0a214a240f34559394cca116c609d5bbf670ed85c7b983f0026154278bffd2b53d8aea4735ed99c39ea45db004c16bee078bb0b40e38ae510cacd1955a4e3eb90347d344cdcce07bddb89d9cd2077558914179a8157a87eac86e1b1a07a3f697a5f3f6512e276741d76bcc0c4809117c279fbd55d8c2b3d70468fbe4869394d9f2740bcccdf727da10c06de5c6a0d2f893bce078e058604726d32ab17e3b113a3dcbe0c22f2532738cae8cc5fa98c6b8306680b07ef8f0fca5d5910b0203010001300d06092a864886f70d01010505000382010100361152e42ece11bfd72e5795c9e91079b39c5280e30e3394671ca108fd7de9c3cebef2fc2f5ba752664ba44fcddaf49e91a1d7683cafdc11275fa7c1487ae78a659a8dae5d696cd93de810c67f127568dfa60c1962ec5ad2a3ea0560f75ad4a2ea9d388d4497b561242f090de2d3347dd32494ba6305735fa21d82f037f4355583fdfb1f46a56c19526969ba5f7f556cca9b9069cd9a9e3cd566d2b8c33138609e8794fb0abb11d33ed2c507f7f7df9ce24b3b64713ccdf2450bb5ec4efedba541dce271c8b3759b340b0467c06624cd3881b769a1d4a1b1fc0bec97d6b8561b032089ab8ca108595759bbd9b95fd43a3d28f518fb9d193125c8fa9b224f831c
3f2ae9c1894282b5e0222f0d06bbf457191f816f
mfDIsnw62VUq5CrwQygwwDHX4oFb9NZomMa1Qv0blGOGPAtzm7d2+whMgYfVEkXw
tm6XtP5M5qvCs+TffoCZhF/AF3Fx7Ow8iqgApPbgXSw=
FfddiHmPb383DV6rreW8JKkRsedppg8iNKEfTaDysv4=
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
f5c59ddbecbef72da9ee9e6cb8b2be23
r05ido8PpVZ2h2V1HWb8y18UjWvZxnyZOvYK4Y06JVkYZsi7FS/S9aZJacgWNWb+
3ad378b027fe45aa8bfbc5bacf56344e

POSSIBLE SECRETS
E72409364B865B757E1D6B8DB73011BBB1D20C1A9F931ADD3C4C09E2794CE102F8AA7F2D50EB88F9880A576E6C7B0E95712CAE9416F7BACB798564627846E93B
JbQbUG5JMJUoI6brnx0x3vZF6jilxsapbXGVfjhN8Fg=
3pegtvj7nkb7e3rwh5b+3dnQATJj6aqtaosJ3DkOYPzNGN2w+CoarbJEsY1UQgeA
8741b0e1a67d6a5421683ff78bddc1ed
919afcc635fd11ea817c025656b09b22
115792089210356248762697446949407573529996955224135760342422259061068512044369
c334ae83accfebb8da23104450c896463c9cfab7
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78
c84d23ade98552f1cec71088c1f0794c
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
5e8f16062ea3cd2c4a0d547876baa6f38cabf625
jtcoe3puh462k3igthcrkmi918i30edh47c1tksma0pe1uqmuhc2o7i3g7ansalg
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
baddd789a5e547a19ec8453061580c97
8f1d08a2d6496191a5ebae8f0590f513e2619489

POSSIBLE SECRETS
714075a59dd34064985c7da5ccbfcee4
d225547d92b743179d8a04b75bf7d116
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
953154ac4464acdcdc8f392f879c5bd5798cd286
a0afd19316b54fbaa328a8841fa6722c
3ps9rI142V56fUZ22VD6Aav/U6wPd6aBlBvFChUyHGs=
9b8f518b086098de3d77736f9458a3d2f6f95a37
ace60f6352f6dd9289843b5b0b2ab3d4
lQFXQNWHSdYD6r5tE84uy22hnfx5d1uQHcaULCOPbM14F5cpADjDJSLZMM39MwXu
2OUUc7NT0WkEjmK9+FJMealFwLTaZNBfYG9mkUVQmhidcpLE5upPJKg2uqM0WUBe
Wd8xe/qfTwq3ylFNd3IpaqLHZbh2ZNCLluVzmeNkcpw=
B9q/kZ3M4smaULlSVckwEJdUNHNhTESXBf44c8ZRnHeQQYAcBESnaqAhjIPahrI0
E112a13984c2eF19DBeE98E3eDa79e90DB51f0e6
pJdDeMB2kv4XBHX5K3sZ2yiaFa+GF7/AJrrVARYf41I=
WPHSlfekhaYlGJ3yiaIbiBY4HTx7YM9tPghNjV2alPYI+KXTjj+VnW7A1O7Euzu8

POSSIBLE SECRETS
7VR2YqvFgyvOhGA7139KYJuSHHdzdCxudZ7JSzwex/E=
dc015cfef9194cefa8b52114a6468262
cc2751449a350f668590264ed76692694a80308a
pORZNbNq0Oj61ZjvW9kWzatiK7LMxOR6JjGIN24dRVcLieCRVYuov8581WrmSeOY
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
BYT/lgG9eBlnAgDZzPD0oHgzdaaxxy72moL0pisX7NM=
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
tJgqVBYK8iACgXDpES6chgsdiLTk4pCmM15TE0z3kgM=
kd3av/xIh4WVmhBCVqo9sHJVJ1Nfp9EEBESbqmCB4V8=
115792089210356248762697446949407573530086143415290314195533631308867097853951
C10F7968CFE2C76AC6F0650C877806D4514DE58FC239592D2385BCE5609A84B2A0FBDAF29B05505EAD1FDFEF3D7209ACBF34B5D0A806DF18147EA9C0337D6B5B
WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18=
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
syWhPUhrPj9a+Sk0yzwWVrNh+MlfsynriPZ0XF+UPwU=

POSSIBLE SECRETS
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
5c3740647e5ea02b8e3a688a
zu6uZ8u7nNJHsIXbotuBCEBd9hieUh9UBKC94dMPsF422AtJb3FisPSqZI3W+06A
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
RLH60+LqkTN+fFoMkyZr3rdaQt8CbwdFGeiAHk8G/Y1GpQIgUmMEvr7Qzmd4S0T8
e3NEybi6UG3v8IfP2IiRsp6KKM0H99WDhy4AYfUmNolCq+mgpr0V0zn7xdgcLXPM
9bH7YEZYe5itvs31c1gcj+rhSSdPNkSIQfDNYXo9ahs=
RDFKlEPOT0aQT6ARmaMKbVy+V0L7x+JIeY4JSh39pzY=
KF7kIGwoAULxxzCbY3v7c6qTHz0AzEhtAn+fEEmtiVY=
3jRp5GOI+HfffIZaNgs5urp4INMy6m1jZanprlp8fEbfjaITI/GTtSmO29P018Ft
Tx+r89A46YvA23pzmXogrUOA3X/vGVWSwDDb1CKb3SB+k9Zvmo8EcgSe2zWDveRy
4a53881e97f34222a385c4b4073ee2b7
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

Report Generated by - MobSF v4.0.3

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