MOBSF

ANDROID STATIC ANALYSIS REPORT

Aptoide (9.21.0.1)

File Name:	easy-emi-loan-calculator.apk
Package Name:	cm.aptoide.pt
Scan Date:	July 7, 2024, 5:02 p.m.
App Security Score:	18/100 (CRITICAL RISK)
Grade:	
Trackers Detection:	6/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
47	24	2	1	2

FILE INFORMATION

File Name: easy-emi-loan-calculator.apk
Size: 20.43MB
MD5: 172c7ab888ea6ddb5c1f19c26e0e7c8c
SHA1: 95fc9e8f5b1a3fba4b5ad7850c5e714c4b6741bc
SHA256: 8b009350a21e045cd9c6a14f0447a6696bb19f7d95cc046699b827441064ee09

APP INFORMATION

App Name: Aptoide
Package Name: cm.aptoide.pt
Main Activity: cm.aptoide.pt.view.MainActivity
Target SDK: 29
Min SDK: 16
Max SDK:
Android Version Name: 9.21.0.1

Android Version Code: 12025

APP COMPONENTS

Activities: 11
Services: 10
Receivers: 14
Providers: 6
Exported Activities: 2
Exported Services: 3
Exported Receivers: 4
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MODEL check Build.PRODUCT check possible Build.SERIAL check network operator name check device ID check FINDINGS: Compiler — DETAILS: r8

<table>
<tr><th>FILE</th><th>DETAILS</th></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
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>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></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://, aptoideinstall://, aptoideauth://, aptoidesearch://, aptoidefeature://, market://, https://, Hosts: app.aptoide.com, market.android.com, webservices.aptoide.com, play.google.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, *.jp.aptoide.com, *.kr.aptoide.com, *.ua.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, jp.aptoide.com, kr.aptoide.com, ua.aptoide.com, community.aptoide.com, become-a-power-gamer.aptoide.com, Mime Types: application/vnd.cm.aptoide.pt, Path Prefixes: /apkinstall, Path Patterns: /store/..*, /thank-you*, /appcoins, /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: 14 | 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	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.
5	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.
6	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.
7	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.

NO	ISSUE	SEVERITY	DESCRIPTION
8	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.
9	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.

NO	ISSUE	SEVERITY	DESCRIPTION
10	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.
11	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.

NO	ISSUE	SEVERITY	DESCRIPTION
12	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: 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.
13	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.

NO	ISSUE	SEVERITY	DESCRIPTION
14	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.
15	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.

NO	ISSUE	SEVERITY	DESCRIPTION
16	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.
17	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.

NO	ISSUE	SEVERITY	DESCRIPTION
18	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.
19	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.

NO	ISSUE	SEVERITY	DESCRIPTION
20	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.
21	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.

NO	ISSUE	SEVERITY	DESCRIPTION
22	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.
23	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.

NO	ISSUE	SEVERITY	DESCRIPTION
24	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.
25	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.

NO	ISSUE	SEVERITY	DESCRIPTION
26	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.
27	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.

NO	ISSUE	SEVERITY	DESCRIPTION
28	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.
29	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.

NO	ISSUE	SEVERITY	DESCRIPTION
30	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.
31	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.

NO	ISSUE	SEVERITY	DESCRIPTION
32	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.
33	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.

NO	ISSUE	SEVERITY	DESCRIPTION
34	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.
35	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.

NO	ISSUE	SEVERITY	DESCRIPTION
36	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.
37	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.

NO	ISSUE	SEVERITY	DESCRIPTION
38	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.
39	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.

NO	ISSUE	SEVERITY	DESCRIPTION
40	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.
41	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.

NO	ISSUE	SEVERITY	DESCRIPTION
42	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.
43	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.

NO	ISSUE	SEVERITY	DESCRIPTION
44	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://jp.aptoide.com]	high	App Link asset verification URL (http://jp.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.
45	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://kr.aptoide.com]	high	App Link asset verification URL (http://kr.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
46	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://ua.aptoide.com]	high	App Link asset verification URL (http://ua.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.
47	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
48	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.
49	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://become-a-power-gamer.aptoide.com]	high	App Link asset verification URL (http://become-a-power-gamer.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
50	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=https://become-a-power-gamer.aptoide.com]	high	App Link asset verification URL (https://become-a-power-gamer.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.
51	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.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
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	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.

NO	ISSUE	SEVERITY	DESCRIPTION
58	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.
59	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: 0 | WARNING: 8 | INFO: 1 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	cm/aptoide/pt/BuildConfig.java cm/aptoide/pt/database/room/RoomNotification.java cm/aptoide/pt/database/room/RoomStore.java cm/aptoide/pt/dataprovider/model/v3/CheckUserCredentialsJson.java cm/aptoide/pt/preferences/LocalPersistenceAdultContent.java cm/aptoide/pt/preferences/managed/ManagedKeys.java cm/aptoide/pt/themes/ThemeManager.java com/aptoide/aptoide_ab_testing/model/Distribution.java com/aptoide/aptoide_ab_testing/model/EvalContext.java com/aptoide/aptoide_ab_testing/model/Flag.java com/aptoide/aptoide_ab_testing/model/PostEvaluationResponseJson.java com/aptoide/aptoide_ab_testing/model/Variant.java com/bumptech/glide/load/engine/d.java com/bumptech/glide/load/engine/p.java com/bumptech/glide/load/h.java p/b/l/g/k.java
				cm/aptoide/aptoideviews/common/StringUtilsKt.java cm/aptoide/pt/crashreports/CrashReport.java cm/aptoide/pt/install/installer/Root.java cm/aptoide/pt/install/remote/RemoteI

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	nstallationSenderManager.java cm/aptoide/pt/logger/Logger.java cm/aptoide/pt/root/RootShell.java cm/aptoide/pt/root/containers/RootClass.java com/airbnb/epoxy/i.java com/airbnb/lottie/c.java com/airbnb/lottie/d.java com/airbnb/lottie/l.java com/airbnb/lottie/r/a.java com/airbnb/lottie/r/b.java com/aptoide/aptoide_ab_testing/model/EvalDebugLog.java com/aptoide/aptoide_ab_testing/model/SegmentDebugLog.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/i.java com/bumptech/glide/load/engine/b0/a.java com/bumptech/glide/load/engine/b0/b.java com/bumptech/glide/load/engine/z/j.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/e.java com/bumptech/glide/load/n/c.java com/bumptech/glide/load/n/t.java com/bumptech/glide/load/o/c/j.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/m/e.java com/bumptech/glide/m/f.java com/bumptech/glide/m/n.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/n/d.java com/bumptech/glide/p/l/j.java com/bumptech/glide/q/a.java com/bumptech/glide/r/l/a.java io/rakam/api/i.java k/a/k/a/a.java k/h/e/c.java k/h/e/g.java k/h/e/k.java k/h/j/b.java k/h/k/b.java k/h/l/b.java k/h/l/d0.java k/h/l/e0/c.java k/h/l/f.java k/h/l/h.java k/h/l/v.java k/h/l/w.java k/h/l/y.java k/j/a/c.java k/l/b/c.java k/m/a/a.java k/n/a.java k/n/b.java k/o/a/b.java k/q/a/c.java k/s/i0.java k/s/y.java m/b/a/a/a.java m/e/b/b/m/h.java m/e/b/b/w/d.java m/e/b/b/x/b.java m/f/a/a/a.java p/b/g/a.java
3	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	k/n/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/liulishuo/filedownloader/services/c.java
5	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	cm/aptoide/pt/utils/AptoideUtils.java io/sentry/connection/l.java
6	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/utils/AptoideUtils.java m/h/a/f0/f.java
7	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
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/flurry/sdk/l1.java
9	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/database/room/RoomInstalled.java com/flurry/sdk/i4.java
10	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	cm/aptoide/pt/BuildConfig.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	5/45	com.android.launcher.permission.INSTALL_SHORTCUT, android.permission.AUTHENTICATE_ACCOUNTS, android.permission.REQUEST_INSTALL_PACKAGES, android.permission.FOREGROUND_SERVICE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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

🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
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
docs.sentry.io	ok	**IP:** 76.76.21.98 **Country:** United States of America **Region:** California **City:** Walnut **Latitude:** 34.015400 **Longitude:** -117.858223 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
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

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
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
www.youtube.com	ok	**IP:** 216.58.210.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.aptoide.com	ok	**IP:** 54.170.100.54 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sentry.aptoide.com	ok	**IP:** 52.208.211.210 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **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
cdn6.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
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
catappult.io	ok	**IP:** 3.164.68.122 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api.indicative.com	ok	**IP:** 34.98.104.50 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

EMAILS

EMAIL	FILE
485bb7b111d41f17e0f8@sentry.aptoide	cm/aptoide/pt/BuildConfig.java
suport@aptoide.com aptoide@aptoide.com support@aptoide.com □□□suport@aptoide.com□□□□□□□	Android String Resource

TRACKERS

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
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

🔑 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"

POSSIBLE SECRETS
"com_facebook_device_auth_instructions" : "facebook.com/device□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"nothing_inserted_user" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"password" : "□□□□□□"
"recover_password" : "□□□□□□□□□□□□□□□□□□"
"store_username" : "□□□□□□□"
"username" : "E□□□"
"password" : "■■■■■■"
"store_username" : "■■■■■"
"username" : "■■■■"
"password" : "Passwort"
"store_username" : "Nick"
"username" : "E-Mail"
"password" : "Парола"
"store_username" : "Прякор"
"username" : "Имейл"

POSSIBLE SECRETS
"nothing_inserted_user" : "[redacted]"
"password" : "[redacted]"
"recover_password" : "[redacted]"
"social_timeline_users_private" : "%d[redacted]"
"store_username" : "[redacted]"
"username" : "[redacted]"
"password" : "Salasana"
"store_username" : "Nimimerkki"
"username" : "Sähköposti"
"password" : "[redacted]"
"store_username" : "[redacted]"
"store_username" : "Nickname"
"password" : "Пароль"
"store_username" : "Псевдонім"
"store_username" : "Ψευδώνυμο"

POSSIBLE SECRETS
"username" : "Email"
"password" : "Wachtwoord"
"store_username" : "Weergavenaam"
"username" : "E-mail"
"password" : "Hasło"
"store_username" : "Pseudonim"
"username" : "Email"
"password" : "[redacted]"
"store_username" : "[redacted]"
"username" : "[redacted]"
"username" : "Email"
"password" : "□□□□"
"store_username" : "□□"
"username" : "□□□"
"password" : "Parolă"

POSSIBLE SECRETS
"store_username" : "Pseudonim"
"username" : "E-mail"
"store_username" : "Pseudo"
"username" : "Email"
"password" : "[redacted]"
"username" : "[redacted]"
"password" : "Lozinka"
"store_username" : "Nadimak"
"username" : "E-pošta"
"password" : "Şifre"
"username" : "E-posta"
"password" : "Contraseña"
"store_username" : "Apodo"
"username" : "E-mail"
"username" : "E-mel"

POSSIBLE SECRETS
"password" : "Password"
"store_username" : "Nickname"
"password" : "Palavra-passe"
"store_username" : "Alcunha"
"username" : "E-mail"
"password" : "Jelszó"
"store_username" : "Becenév"
"username" : "E-mail"
"password" : "Пароль"
"store_username" : "Никнейм"
"username" : "E-mail"
"password" : "[redacted]"
"store_username" : "[redacted]"
"username" : "[redacted]"
"com_facebook_device_auth_instructions" : "[redacted]facebook.com/device[redacted]"

POSSIBLE SECRETS
"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□□□□□□□□□□□□□□"
"password" : "□□"
"recover_password" : "□□□□□□□"
"store_username" : "Nickname"
"username" : "□□□□□"
"com_facebook_device_auth_instructions" : "□□<b>facebook.com/device</b&gt□□□□□□□□□□□□□□"
JbQbUG5JMJUoI6brnx0x3vZF6jilxsapbXGVfjhN8Fg=

POSSIBLE SECRETS
308203643082024ca0030201020204503fc625300d06092a864886f70d01010505003073310b3009060355040613027074311030 0e06035504081307556e6b6e6f776e310f300d060355040713064c6973626f6e3115301306035504a130c4361697861204d6167696361311030 10f300d060355040713064c6973626f6e3115301306035504a130c4361697861204d6167696361311030e060355040b13074170746f6964653118301606035504031 0f447561727465205369 6c76656972613020170d313230383330313935393335a180f32303934313031393139353933335a3073310b3009060355040613027074311030 00e06035504081307556e6b6e6f776e310f300d060355040713064c6973626f6e3115301306035504a130c4361697861204d6167696361311030e060355040b130741 70746f6964653118301606035504031 30f447561727465205369 6c76656972613082012230 0d06092a864886f70d01010105000382010f003082010a0282010100a7032c b40819b62cd596bc1c121951724e9a7d6612222d63dab58a18970339f77911b8e2a0665aa15efb051d4dd710c99e1fcaea006a651b7c113a71649c315e27122b9e0a214a 240f34559394cca116c609d5bbf670ed85c7b983f0026154278bffd2b53d8aea4735ed99c39ea45db004c16bee078bb0b40e38ae510cacd1955a4e3eb90347d344cdcce07 bddb89d9cd2077558914179a8157a87eac86e1b1a07a3f697a5f3f6512e276741d76bcc0c4809117c279fbd55d8c2b3d70468fbe4869394d9f2740bcccdf727da10c06de5c 6a0d2f893bce078e058604726d32ab17e3b113a3dcbe0c22f2532738cae8cc5fa98c6b8306680b07ef8f0fca5d5910b0203010001300d06092a864886f70d0101050500038 2010100361152e42ece11bfd72e5795c9e91079b39c5280e30e3394671ca108fd7de9c3cebef2fc2f5ba752664ba44fcddaf49e91a1d7683cafdc11275fa7c1487ae78a659a 8dae5d696cd93de810c67f127568dfa60c1962ec5ad2a3ea0560f75ad4a2ea9d388d4497b561242f090de2d3347dd32494ba6305735fa21d82f037f4355583fdfb1f46a56c 19526969ba5f7f556cca9b9069cd9a9e3cd566d2b8c33138609e8794fb0abb11d33ed2c507f7f7df9ce24b3b64713ccdf2450bb5ec4efedba541dce271c8b3759b340b0467 c06624cd3881b769a1d4a1b1fc0bec97d6b8561b032089ab8ca108595759bbd9b95fd43a3d28f518fb9d193125c8fa9b224f831c
SVqWumuteCQHvVIaALrOZXuzVVVeS7f4FGxxu6V+es4=
cAajgxHIj7GTSEIzIYIQxmEIoOSoJq7VOaxWHfv72QM=
WoiWRyIOVNa9ihaBciRSC7XHjIiYS9VwUGOIud4PB18=

POSSIBLE SECRETS
308205653082034ca00302010202044df76b53300d06092a864886f70d01010505003073310b30090603550406130270743110300e06035504081307556e6b6e6f776e310f300d060355040713064c6973626f6131153013060355040a130c4361697861204d61676963613110300e060355040b1307556e6b6e6f776e311830160603550403130f4475617274652053696c76656972613020170d3131303631343134303831395a180f32303933303830323134303831395a3073310b30090603550406130270743110300e06035504081307556e6b6e6f776e310f300d060355040713064c6973626f6131153013060355040a130c4361697861204d61676963613110300e060355040b1307556e6b6e6f776e311830160603550403130f4475617274652053696c766569726130820222300d06092a864886f70d01010105000382020f003082020a02820201026cfe7512fa0c40520971ee83e227208e072a1e1962a4fd0cd5c709e33dc45ce856e9ddc2b9a918394e96ec462d5fea2db81c443b9dbedd75a1031a1f1593b86eef83302f9ecdc0dfd227a3e11ccedb056e58c79b9177dbefba122a390dac88a90a317cb55a9171ab428b46c2e29b5d7fef2e823f5985b9c165a1edba7c82b4f8d5e3aa346996019cb8b7bcc768f5fdae15975add5e53c1fc022e4c99dababf3a80c5a09680ba4b8889cc4399940d92d11c289268d3f2671b98f871964f21c5870d9a1c72c8fbea65a637a06643f246e733fff37b7db4020fd2b6e7343fdbac2ddd20f8a48710d944d8f76432a3225f72c6a50c4e76247fb9256f294eeb9e24080ad28094fbfcfa6e4b5a85d652b1c5d967b39ee1272955a134a0ff1e89bb01f98d710204c72ca4c9dd44ecdd81358a8ef920fa371edd1bfc097c81678aa31b059b9218eba5c0ed2c209bd799a3ecab19e5e3b0e3d18029bf156b37e091969b4e5ae5024475b038b4d841e0e88580fd433154f606f1f7c14527f00509dd7448911e1ec44cb1e94f7dce59459e95438c4a245103d14fff047f97d14bf38f1802d84727b0f3aa98e02e8840892c629e303f76965e186de1d92263ec17e35aa224c33856d59095cf9195042ebfb5fd4703ef8add7ccf923640f266c22e432232f5c6b0873d99ebd509f9e66a77506eabef04ae1d9cf5edb40e13bc1cff39917da8b70203010001300d06092a864886f70d01010505000382020200069a29624d30983fdec4c4bf685f2f479214fda52e272a74ae8aee8bc7aae441ba79977cdd251cf5b21c56ee631dd1e17da28a2bd87d1190b4c1cc440140251e38af40aa694e6d3965c31b36ade9deccde0ca403639031f44f42e395b575a125cd210fd54e9ac760af1ed72c7b91f8f771074f6cafe0d28ab840510ee98a46eb84225be218ff6f90d036f47ec2e7dbfa067e9498cc633e5cab354ab86013b4d8047312643cdfbb6b3654dc26a87af0f4d83b2b0c6ad28d026483788daeda241c8e2631311e0e0d48c6f9284904cc4df114336c207e4c4f468f80f82f2d6917d8ec6b9e63fa2a0f126f668f8220667c92d26d55b5da7a4144b8693c0dec479a3c63b1d43eb96868eac1cb786e2f4b327bad553fc9ffe2dada3ab11bd6b1d7a623a92e821192b0dbcdabf0e4c361561bb5abb970d11e477050d56957fc8961106d2aaf1f209cbdde733a7a6e0577fd35d32f048e887b0e92c9415871e5b0d7458fe682256494b6c9443d04a076842d56374ee4c184a5c64a71c6818eafaa6dcbd66aae917907080d4895b7b0c941a4fae00be891666c0bdeb8b9331d0ff61d7ec2c26b80156aa64263e925dc9d84279bdb1e27e0403b57c14a1b2647a98c858ee20c92b967fb1eb963147fe390958e7c914fce69e1e2eb06139279b70a8eeabe99500ddf04223c3343e5c9b2722635856c65593aae9d2dbf3da704f79e8145f008e
B3EEABB8EE11C2BE770B684D95219ECB
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
305bdd41-271f-4618-a1ea-0793da9e04ef
919afcc635fd11ea817c025656b09b22
1b2ec33c1a5a485bb7b111d41f17e0f8
jtcoe3puh462k3igthcrkmi918i30edh47c1tksma0pe1uqmuhc2o7i3g7ansalg

POSSIBLE SECRETS
uUwZgwDOxcBXrQcntwu+kYFpkiVkOaezL0WYEZ3anJc=
3ad378b027fe45aa8bfbc5bacf56344e
Wd8xe/qfTwq3ylFNd3IpaqLHZbh2ZNCLluVzmeNkcpw=
UZJDjsNp1+4M5x9cbbdflB779y5YRBcV6Z6rBMLIrO4=

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.