MOBSF

ANDROID STATIC ANALYSIS REPORT

Salto KS (8.17.0)

File Name:	nl.moboa.myclay.apk
Package Name:	nl.moboa.myclay
Scan Date:	Jan. 3, 2026, 6:13 a.m.
App Security Score:	47/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
6	30	4	3	2

FILE INFORMATION

File Name: nl.moboa.myclay.apk
Size: 15.23MB
MD5: c24c5f335adbb47c489bbd2aa9a5fb67
SHA1: d135145f3ad79615d675e3a47e5baba2e0381ee4
SHA256: 92d0def75519738622b5228c612f5fa54c5db3961e319f34907ad0eda5a46783

APP INFORMATION

App Name: Salto KS
Package Name: nl.moboa.myclay
Main Activity: nl.moboa.myclay.main.AnimationActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 8.17.0

Android Version Code: 2013000215

APP COMPONENTS

Activities: 108
Services: 15
Receivers: 16
Providers: 7
Exported Activities: 10
Exported Services: 3
Exported Receivers: 5
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=NL, ST=ZH, L=Rotterdam, O=Moboa, CN=Bart Jochems
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-01-24 17:07:35+00:00
Valid To: 2038-01-18 17:07:35+00:00
Issuer: C=NL, ST=ZH, L=Rotterdam, O=Moboa, CN=Bart Jochems
Serial Number: 0x51016a57
Hash Algorithm: sha1
md5: 18cf7e2a78c7138781faf76828cebf6c
sha1: 729a017c741d5ad6b51b59a62ea8d4239a391378
sha256: 39eb36affec6edd5b5e9df96a217a31faca928ed5931c8c6de90fa402a616652
sha512: d4bb62660cddfdd76c239de713a108e467a1f02d0f04d5f44d47caed572d1e182117c1eda4245c57c2d961d2d26c55e23b8ed0961a86b6732a76387e4887abbc
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: cbf37b1bf44f60a52e7f7d929dc07b3658ad974451f9e3e939c1c7f3b0172ca0
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
nl.moboa.myclay.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
nl.moboa.myclay.permission.UA_DATA	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE_MICROPHONE	normal	permits foreground services with microphone use.	Allows a regular application to use Service.startForeground with the type "microphone".
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.FOREGROUND_SERVICE_PHONE_CALL	normal	enables foreground services during phone calls.	Allows a regular application to use Service.startForeground with the type "phoneCall".
android.permission.MANAGE_OWN_CALLS	normal	enables a calling app to manage its own calls.	Allows a calling application which manages it own calls through the self-managed ConnectionService APIs.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
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.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.providers.gsf.permission.READ_GSERVICES	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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
nl.moboa.myclay.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check Build.TAGS check SIM operator 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.HARDWARE check
Build.BOARD check
Build.TAGS check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>res/raw/android_wear_micro_apk.apk!classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.BOARD check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
nl.moboa.myclay.main.AnimationActivity	Schemes: file://, content://, https://, Hosts: *, www.saltoks.com, Mime Types: application/x-*, application/xml, application/postscript, application/plain, application/x-tcl, application/x-javascript, application/inf, application/octet-stream, text/*,
nl.moboa.myclay.main.MainActivity	Schemes: stonly-avbpe3poz2://,
net.openid.appauth.RedirectUriReceiverActivity	Schemes: nl.moboa.myclay://,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

NETWORK SECURITY

HIGH: 0 | WARNING: 0 | INFO: 0 | SECURE: 0

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: **3** | WARNING: **18** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	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	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	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
4	App Link assetlinks.json file not found [android:name=nl.moboa.myclay.main.AnimationActivity] [android:host=https://www.saltoks.com]	high	App Link asset verification URL (https://www.saltoks.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.
5	Activity (nl.moboa.myclay.main.MainActivity) 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.
6	Activity (nl.moboa.myclay.login.LoginActivity) 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.
7	Activity (nl.moboa.myclay.login.LoginPrefilledActivity) 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.
8	Activity (nl.moboa.myclay.widget.ClayAppWidgetPermissionActivity) 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.
9	Activity (nl.moboa.myclay.mkey.guest.GuestDigitalKeyRetrievalActivity) 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	Activity (nl.moboa.myclay.legal.SaltoLegalInitialActivity) 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
11	Service (nl.moboa.myclay.messaging.ClayMessagingService) is not Protected. [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.
12	Service (nl.moboa.myclay.application.ClayHceService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NFC_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.
13	Broadcast Receiver (nl.moboa.myclay.widget.ClayAppWidgetProvider) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
14	Activity (net.openid.appauth.RedirectUriReceiverActivity) 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.
15	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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.
16	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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
17	Broadcast Receiver (com.pusher.pushnotifications.reporting.FCMMessageReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
18	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
19	Activity (androidx.compose.ui.tooling.PreviewActivity) 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.
20	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.

NO	ISSUE	SEVERITY	DESCRIPTION
21	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
22	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: **2** | WARNING: **10** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A3/a.java B/m.java B3/a.java B3/b.java C3/a.java C3/b.java C3/c.java C3/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				C3/d.java C4/g.java C9/C0064e.java D3/d.java D3/g.java E2/r.java E3/a.java E3/c.java E3/d.java E3/e.java F3/a.java F5/b.java Fg/C0166n.java G5/b.java G5/c.java I/x.java J1/a.java J1/e.java L1/c.java M4/c0.java M7/d.java M7/u.java N2/g.java O2/f.java O2/m.java O2/n.java Og/l.java P1/b.java P6/a.java Pg/d.java Q5/c.java Q7/b.java R0/d.java R1/AbstractC0578p.java R1/C0574l.java R1/C0575m.java T0/e.java T0/p.java T1/d.java T1/k.java U9/J.java V0/f.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	V0/f.java V2/b.java V2/e.java V2/f.java W/e.java Y1/e.java Y5/a.java Yc/c.java Z0/B.java Z0/p.java Z5/d.java Z5/j.java Zg/h.java a2/C0801c.java a2/J.java a2/O.java a8/AbstractC0872s.java b2/C1036a.java c3/h.java com/comelitgroup/module/ModuleService.java com/comelitgroup/module/notification/NotificationActionReceiver.java com/comelitgroup/module/receivers/NetReceiver.java com/comelitgroup/module/ui/call/CallActivity.java com/comelitgroup/module/ui/call/CfpActivity.java com/comelitgroup/vipcomelit/VipComelitEngine.java com/journeyapps/barcodescanner/CameraPreview.java com/journeyapps/barcodescanner/CaptureActivity.java com/pusher/pushnotifications/logging/Logger.java com/stonly/stonly/core/TrackerInteractor.java com/stonly/stonly/parser/compose/CssSelectorComposeMatcher.java com/stonly/stonly/trigger/TriggerInte

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/stonly/stonly/trigger/TriggerInteracter$triggers$1.java com/stonly/stonly/widget/BaseWidgetInteractor$sanitizeData$1.java com/stonly/stonly/widget/BaseWidgetView.java com/stonly/stonly/widget/WidgetExtKt.java com/virgilsecurity/crypto/common/utils/NativeUtils.java e/C1345j.java e6/C1414h.java f/C1471d.java f3/C1487a.java g7/C1624g.java h/AbstractC1706q.java h/C1683S.java h/C1693d.java h/C1714y.java h/C1715z.java h/LayoutInflaterFactory2C1669D.java h/RunnableC1676K.java h/RunnableC1681P.java io/sentry/C1881m0.java io/sentry/android/core/I.java k/C1985h.java l/ViewOnKeyListenerC2094j.java l3/C2105a.java l3/c.java l3/h.java l3/j.java l3/l.java m3/C2168b.java m3/f.java n1/m.java n9/c.java n9/e.java nl/moboa/myclay/application/MyClayApplication.java o2/C2368j.java o2/C2380v.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o3/C2385a.java o6/n.java o9/AbstractC2429c.java o9/C2428b.java o9/RunnableC2430d.java o9/e.java o9/g.java o9/h.java o9/k.java o9/m.java org/joda/time/tz/DateTimeZoneBuilder.java org/joda/time/tz/ZoneInfoCompiler.java p/o.java p3/b.java p3/c.java r/C2807d.java r3/CallableC2815a.java r3/CallableC2816b.java r3/CallableC2817c.java r3/CallableC2818d.java s1/AbstractC2893h0.java s1/AbstractC2901l0.java s1/l0.java s1/r.java t6/C3025a.java t7/C3036d.java u/g.java w3/RunnableC3318a.java wb/H.java x2/f.java x7/f.java y1/C3588k.java y1/r.java z5/C3699c.java z7/m.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	Ad/w.java C9/C0064e.java Oe/d.java Y5/a.java Z5/d.java Z5/i.java Z5/j.java a6/C0839f.java a6/C0847n.java c3/h.java com/comelitgroup/module/provider/ContentVipProvider.java f3/C1487a.java f3/b.java i2/C1776b.java l3/C2105a.java m3/C2168b.java
3	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	C4/g.java io/sentry/android/core/z.java
				J/C0367j0.java M4/A.java M4/C.java M4/C0454l.java M4/C0467z.java M4/D.java M4/E.java M4/G.java M4/Q.java N2/d.java com/pusher/pushnotifications/internal/DeviceStateStore.java com/pusher/pushnotifications/internal/InstanceDeviceStateStore.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/pusher/pushnotifications/reporting/ReportingWorker.java com/stonly/stonly/BuildConfig.java
4	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/stonly/stonly/data/BuildConfig.java com/stonly/stonly/data/TrackerRepository.java com/stonly/stonly/data/TriggerRepository.java com/stonly/stonly/utils/BuildConfig.java nl/moboa/clayservice/filter/constants/ODataGroups.java nl/moboa/clayservice/models/eagleEye/camera/CameraInfo.java nl/moboa/clayservice/models/error/ResourceError.java nl/moboa/clayservice/models/mkey/DKeyBaseInfoMessage.java nl/moboa/clayservice/models/mkey/WearOSMKeyInfoMessage.java nl/moboa/myclay/ble/list/wifi/WiFiCredential.java nl/moboa/myclay/migration/models/MigratedIQActivation.java nl/moboa/myclay/utils/SharedPreferencesUtil.java o8/C2423a.java pa/C2623k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	Dd/c.java Og/d.java Og/g.java Og/k.java Og/l.java Zc/i.java Zc/j.java com/pusher/pushnotifications/api/PushNotificationsAPI.java com/pusher/pushnotifications/reporting/api/ReportingAPI.java com/stonly/stonly/data/network/ApiManager.java
6	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	Fg/C0166n.java h/RunnableC1676K.java o1/RunnableC2332a.java o5/d.java oa/C2435a1.java oa/C2464i0.java oa/C2470k0.java oa/J1.java pa/C2626n.java q0/C2691X.java tb/AbstractC3041a.java tb/C3042b.java ub/C3129a.java va/u.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	R4/b.java io/sentry/j1.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	Pf/a.java nl/moboa/myclay/pods/activities/SharePodGuestAccessCodeActivity.java q0/C2714k.java
9	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	F6/a.java p/r.java
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	F7/k.java J7/b.java M7/d.java io/sentry/android/core/internal/util/f.java io/sentry/android/core/z.java nl/moboa/myclay/main/AnimationActivity.java nl/moboa/myclay/utils/RootUtil.java
11	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/stonly/stonly/widget/StonlyWebView.java
12	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	com/pusher/pushnotifications/internal/ServerSyncProcessHandler.java nl/moboa/clayservice/models/IQSecret.java
13	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
14	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/stonly/stonly/di/StonlyModule.java h/RunnableC1676K.java
15	Calling Cipher.getInstance("AES") will return AES ECB mode by default. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	nl/moboa/myclay/utils/AESCrypto.java
16	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	n9/h.java
17	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	V2/b.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00162	Create InetSocketAddress object and connecting to it	socket	Og/c.java Og/l.java

RULE ID	BEHAVIOUR	LABEL	FILES
00163	Create new Socket and connecting to it	socket	Og/c.java Og/l.java
00014	Read file into a stream and put it into a JSON object	file	C4/g.java
00022	Open a file from given absolute path of the file	file	C4/g.java I0/v.java Q5/c.java Y/p.java Y5/a.java e0/C1347a.java i4/C1786e.java io/sentry/C1901u0.java io/sentry/RunnableC1905w0.java io/sentry/android/core/C1842g.java io/sentry/android/core/z.java io/sentry/cache/a.java io/sentry/cache/c.java io/sentry/j1.java io/sentry/r.java j2/C1923a.java n9/h.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	C4/g.java Fg/U.java Hg/f.java Hg/i.java J1/e.java N2/f.java Q7/b.java T6/g.java Y1/b.java Y1/e.java Y1/i.java a8/AbstractC0872s.java e6/AbstractC1412f.java g1/AbstractC1588h.java io/sentry/C1901u0.java io/sentry/Q0.java io/sentry/RunnableC1905w0.java io/sentry/cache/a.java io/sentry/cache/c.java io/sentry/instrumentation/file/c.java io/sentry/r.java j1/h.java j1/i.java j4/C1926b.java k1/c.java l4/k.java org/joda/time/tz/ZoneInfoCompiler.java org/joda/time/tz/ZoneInfoProvider.java
00005	Get absolute path of file and put it to JSON object	file	C4/g.java
00009	Put data in cursor to JSON object	file	C4/g.java N2/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00004	Get filename and put it to JSON object	file collection	C4/g.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	Ad/x.java Fd/b.java Nf/b.java R1/C0563a.java R1/C0565c.java com/stonly/stonly/widget/StonlyWebViewClient.java df/C1325a.java df/C1329e.java dg/ViewOnClickListenerC1334c.java je/AbstractC1964e.java lg/C2147c.java net/openid/appauth/AuthorizationManagementActivity.java nl/moboa/myclay/legal/SaltoLegalInitialActivity.java nl/moboa/myclay/mkey/guest/GuestDigitalKeyWelcomeFragment.java nl/moboa/myclay/settings/ProfileSettingsActivity.java qg/c.java wf/C3360d.java yf/C3671c.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	Ad/x.java Nf/b.java R1/C0563a.java R1/C0565c.java net/openid/appauth/AuthorizationManagementActivity.java nl/moboa/myclay/settings/ProfileSettingsActivity.java wf/C3360d.java yf/C3671c.java
00096	Connect to a URL and set request method	command network	C9/C0064e.java T6/q.java io/sentry/transport/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	C9/C0064e.java T6/q.java io/sentry/transport/g.java
00030	Connect to the remote server through the given URL	network	T6/q.java io/sentry/transport/g.java
00109	Connect to a URL and get the response code	network command	C9/C0064e.java T6/q.java io/sentry/transport/g.java
00094	Connect to a URL and read data from it	command network	T6/q.java
00108	Read the input stream from given URL	network command	T6/q.java
00114	Create a secure socket connection to the proxy address	network command	Jg/j.java
00187	Query a URI and check the result	collection sms calllog calendar	Rf/j.java
00028	Read file from assets directory	file	T6/C0598c.java
00012	Read data and put it into a buffer stream	file	J1/e.java N2/f.java io/sentry/C1901u0.java io/sentry/Q0.java io/sentry/cache/c.java io/sentry/r.java l4/k.java
00079	Hide the current app's icon	evasion	O2/m.java

RULE ID	BEHAVIOUR	LABEL	FILES
00125	Check if the given file path exist	file	Q7/b.java
00036	Get resource file from res/raw directory	reflection	Q7/b.java R1/C0563a.java
00091	Retrieve data from broadcast	collection	H2/c.java X4/c.java com/comelitgroup/module/ModuleService.java net/openid/appauth/AuthorizationManagementActivity.java nl/moboa/myclay/users/UserDetailActivity.java
00075	Get location of the device	collection location	h/C1693d.java
00137	Get last known location of the device	location collection	h/C1693d.java
00183	Get current camera parameters and change the setting.	camera	o9/h.java
00026	Method reflection	reflection	Kb/C.java wb/H.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	U9/p.java
00104	Check if the given path is directory	file	wb/H.java
00112	Get the date of the calendar event	collection calendar	wb/H.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	n9/h.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://my-clay.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/363265004850/namespaces/firebase:fetch?key=AIzaSyAmTAHGPYDAj71WLV7tIRyNybwl9AciM_g. This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	15/25	android.permission.RECORD_AUDIO, android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_PHONE_STATE, android.permission.CAMERA, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_WIFI_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_CONTACTS, android.permission.WRITE_SETTINGS, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.VIBRATE
Other Common Permissions	9/44	android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.CHANGE_NETWORK_STATE, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.CHANGE_WIFI_STATE, com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS

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
www.saltoks.com	ok	**IP:** 98.84.224.111 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
saltoks.page.link	ok	**IP:** 192.178.50.65 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developer.android.com	ok	**IP:** 172.217.2.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app.saltoks.com	ok	**IP:** 20.82.73.88 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
movistarproseguralarmas.es	ok	**IP:** 23.219.2.142 **Country:** Italy **Region:** Sicilia **City:** Catania **Latitude:** 37.502129 **Longitude:** 15.087190 **View:** Google Map
support.saltosystems.com	ok	**IP:** 151.101.130.133 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
issuetracker.google.com	ok	**IP:** 172.217.165.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
s.eagleeyenetworks.com	ok	**IP:** 192.40.4.23 **Country:** United States of America **Region:** Texas **City:** Austin **Latitude:** 30.301081 **Longitude:** -97.814880 **View:** Google Map
my-clay.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
cs.android.com	ok	**IP:** 172.217.2.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
stonly.com	ok	**IP:** 13.35.196.76 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
journeyapps.com	ok	**IP:** 13.35.196.78 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
www.saltosystems.com	ok	**IP:** 151.101.66.133 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cws-fe-38d07.azconfig.ioideiwusecretdwda4afmxkrfziecutlbnohj5wzy1vnkw92w7kxwtlens92ty7apjqqj99baac5rqljdmkwnaaabazac1nga	ok	No Geolocation information available.
github.com	ok	**IP:** 140.82.112.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
saltosystems.com	ok	**IP:** 151.101.2.133 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.stonly.com	ok	**IP:** 13.35.196.76 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.stonly.com	ok	**IP:** 35.180.218.216 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
goo.gle	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map

EMAILS

EMAIL	FILE
support@pusher.com	com/pusher/pushnotifications/internal/ServerSyncProcessHandler.java
john.doe@my-clay.com feedback@saltoks.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
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
"clay_user" : "User"
"comelit_scs_api_configuration" : "comelit_scs_api_configuration"
"eagle_eye_api_key" : "8b315436-64c4-11e8-957f-02420a801302"
"firebase_database_url" : "https://my-clay.firebaseio.com"

POSSIBLE SECRETS
"google_api_key" : "AIzaSyAmTAHGPYDAj71WLV7tIRyNybwl9AciM_g"
"google_crash_reporting_api_key" : "AIzaSyAmTAHGPYDAj71WLV7tIRyNybwl9AciM_g"
"id_login_password" : "password_input"
"id_save_key_button" : "save_key_button"
"id_use_key_button" : "use_key_button"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"mobile_key_widget_url" : "https://saltosystems.com/en/blog/announcing-the-digital-key-widget-for-ios-android/"
"origin_metallickey" : "MetallicKey"
"username" : "Username"
c2f942d2-f84e-11ec-9fb8-0ae9fa2a18a2
b4fd0b02554aa305805c8aa187f9a499d
Secret=DWda4AfmXkRfZiECUtLbnohj5Wzy1Vnkw92W7KXWTLEns92ty7apJQQJ99BAAC5RqLJdMKwnAAABAZAC1Nga
9a04f079-9840-4286-ab92-e65be0885f95
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

POSSIBLE SECRETS
B6E60002-E2E3-BC82-4C72-929D0D29CA17
A022FADD-1900-4B59-8B25-83A1AEE7F65C
B6E60003-E2E3-BC82-4C72-929D0D29CA17
36864200e0eaf5284d884a0e77d31646
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
3071c8717539de5d5353f4c8cd59a032
B6E60001-E2E3-BC82-4C72-929D0D29CA17
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
bae8e37fc83441b16034566b
a898cf86-430f-4369-893c-2d31148149f9
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
d3440605-a126-47eb-8b93-0956bc618bfb
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78

POSSIBLE SECRETS
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
115792089210356248762697446949407573529996955224135760342422259061068512044369
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
2d9f9bec-6031-4b9a-affd-05f53f47a97b
1a934ced-a539-4452-92e4-335406e85cfb
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
5c5a76eb-d3b4-447a-a756-d3ec7a67b3b3
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
572A9214-10DF-4B7D-A7A6-3C193C1309EC
af60eb711bd85bc1e4d3e0a462e074eea428a8

POSSIBLE SECRETS
7d73d21f1bd82c9e5268b6dcf9fde2cb
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3

PLAYSTORE INFORMATION

Title: Salto KS

Score: 3.0350878 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Business **Play Store URL:** nl.moboa.myclay

Developer Details: Salto Cloudworks B.V., Salto+Cloudworks+B.V., None, http://www.saltoks.com/, info@my-clay.com,

Release Date: Apr 2, 2013 **Privacy Policy:** Privacy link

Description:

Salto KS Solution is a smarter way to control your business access. No matter how small your business is, or how big it is. With Salto KS you can manage your business access and see what's happening on your door. The Salto KS Mobile and Wear OS app allows Salto KS users to remotely manage and monitor their door access activity across all their Salto KS systems, as well as: • Swipe-to-Open doors. • Open doors directly from your watch complications. • Block/Unblock user's tags, in case someone lost their keys. • Oversee events on all doors across all systems. • Verify and open doors and block users with Touch ID.

SCAN LOGS

Timestamp	Event	Error
2026-01-03 06:13:13	Generating Hashes	OK

2026-01-03 06:13:13	Extracting APK	OK
2026-01-03 06:13:13	Unzipping	OK
2026-01-03 06:13:13	Parsing APK with androguard	OK
2026-01-03 06:13:13	Extracting APK features using aapt/aapt2	OK
2026-01-03 06:13:13	Getting Hardcoded Certificates/Keystores	OK
2026-01-03 06:13:14	Parsing AndroidManifest.xml	OK
2026-01-03 06:13:14	Extracting Manifest Data	OK
2026-01-03 06:13:14	Manifest Analysis Started	OK
2026-01-03 06:13:15	Reading Network Security config from network_security_config.xml	OK
2026-01-03 06:13:15	Parsing Network Security config	OK
2026-01-03 06:13:15	Performing Static Analysis on: Salto KS (nl.moboa.myclay)	OK

2026-01-03 06:13:16	Fetching Details from Play Store: nl.moboa.myclay	OK
2026-01-03 06:13:16	Checking for Malware Permissions	OK
2026-01-03 06:13:16	Fetching icon path	OK
2026-01-03 06:13:16	Library Binary Analysis Started	OK
2026-01-03 06:13:16	Reading Code Signing Certificate	OK
2026-01-03 06:13:16	Running APKiD 3.0.0	OK
2026-01-03 06:13:19	Detecting Trackers	OK
2026-01-03 06:13:20	Decompiling APK to Java with JADX	OK
2026-01-03 06:13:29	Converting DEX to Smali	OK
2026-01-03 06:13:29	Code Analysis Started on - java_source	OK
2026-01-03 06:13:30	Android SBOM Analysis Completed	OK

2026-01-03 06:13:33	Android SAST Completed	OK
2026-01-03 06:13:33	Android API Analysis Started	OK
2026-01-03 06:13:35	Android API Analysis Completed	OK
2026-01-03 06:13:35	Android Permission Mapping Started	OK
2026-01-03 06:13:57	Android Permission Mapping Completed	OK
2026-01-03 06:13:57	Android Behaviour Analysis Started	OK
2026-01-03 06:14:00	Android Behaviour Analysis Completed	OK
2026-01-03 06:14:00	Extracting Emails and URLs from Source Code	OK
2026-01-03 06:14:04	Email and URL Extraction Completed	OK
2026-01-03 06:14:04	Extracting String data from APK	OK
2026-01-03 06:14:04	Extracting String data from Code	OK

2026-01-03 06:14:04	Extracting String values and entropies from Code	OK
2026-01-03 06:14:05	Performing Malware check on extracted domains	OK
2026-01-03 06:14:08	Saving to Database	OK

Report Generated by - MobSF v4.4.4

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.