ANDROID STATIC ANALYSIS REPORT

app_icon

ClockWork (1.0)

File Name:	ClockWork.apk
Package Name:	com.opsc7311.opsc7311poepart2
Scan Date:	Sept. 1, 2024, 8:41 p.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	7	1	1	0

FILE INFORMATION

File Name: ClockWork.apk
Size: 7.18MB
MD5: ac0a29ec3c32ff663154223905739b7a
SHA1: 28800d58af459dcbf1a2973d4d4453c8a7b29ee9
SHA256: 96f74ee3194cdb6f73699be6c188044f5e5382e3f9d117956a9be5fdaf4d18df

APP INFORMATION

App Name: ClockWork
Package Name: com.opsc7311.opsc7311poepart2
Main Activity: com.opsc7311.opsc7311poepart2.MainActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 7
Services: 1
Receivers: 1
Providers: 2
Exported Activities: 2
Exported Services: 0
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: CN=Nkosinathi Ngozo, O=System sculptors, L=Pretoria, ST=Gauteng, C=RSA
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-09-01 20:30:27+00:00
Valid To: 2049-08-26 20:30:27+00:00
Issuer: CN=Nkosinathi Ngozo, O=System sculptors, L=Pretoria, ST=Gauteng, C=RSA
Serial Number: 0x1
Hash Algorithm: sha256
md5: ff68bc73b86d584866d6379e7b1d1231
sha1: 611fef332157d9977bfeea9989b5aecd20ed76d8
sha256: 070becff76a21626bee030e6e867a6eef1af3c3addb67460147d7c01b72a8369
sha512: 89c283c4d845b15abe7d9c1b240d93dd63a35b24a8c2c4b469d89ff6fe6a88c324570137a0a95ef07b5ea0f62b36abd60b95cb6c22619ef4dc9b9ca129d021ac
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 56be26118369b3227827c383f0702f4d1989173088b84b467123abbbacd9c577
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.opsc7311.opsc7311poepart2.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

FILE	DETAILS
classes2.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check Build.TAGS check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
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

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 4 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched 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	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	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.
4	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
5	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: **0** | WARNING: **2** | INFO: **1** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/ImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java
	The App logs information. Sensitive		CWE: CWE-532: Insertion of	

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	information should never be logged.	info	Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/github/mikephil/charting/charts/BarChart.java com/github/mikephil/charting/charts/BarLineChartBase.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/charts/CombinedChart.java com/github/mikephil/charting/charts/HorizontalBarChart.java com/github/mikephil/charting/charts/PieRadarChartBase.java com/github/mikephil/charting/components/AxisBase.java com/github/mikephil/charting/data/ChartData.java com/github/mikephil/charting/data/CombinedData.java com/github/mikephil/charting/data/LineDataSet.java com/github/mikephil/charting/data/PieEntry.java com/github/mikephil/charting/listener/BarLineChartTouchListener.java com/github/mikephil/charting/renderer/CombinedChartR

NO	ISSUE	SEVERITY	STANDARDS	FILES
				enderer.java com/github/mikephil/charting/renderer/ScatterChartRenderer.java com/github/mikephil/charting/utils/FileUtils.java com/github/mikephil/charting/utils/Utils.java com/opsc7311/opsc7311poepart2/SettingsFragment.java com/opsc7311/opsc7311poepart2/database/service/TimesheetService.java com/opsc7311/opsc7311poepart2/fragments/LeaderboardFragment$getLeaderboard$1.java com/opsc7311/opsc7311poepart2/fragments/LeaderboardFragment$getLeaderboard$2.java com/opsc7311/opsc7311poepart2/fragments/PomodoroFragment.java com/opsc7311/opsc7311poepart2/fragments/TimesheetEntryFragment.java com/opsc7311/opsc7311poepart2/viewmodel/TimesheetViewModel$getTimesheetEntries$1.java
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/manager/RequestManagerRetriever.java com/opsc7311/opsc7311poepart2/database/model/User.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	com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/utils/FileUtils.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	2/24	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	0/45	

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AIzaSyDg1Cx3LL_O9ZJeMl1kzw2SQkuw7zH5HJ0"
"google_crash_reporting_api_key" : "AIzaSyDg1Cx3LL_O9ZJeMl1kzw2SQkuw7zH5HJ0"
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

POSSIBLE SECRETS
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
af60eb711bd85bc1e4d3e0a462e074eea428a8
bae8e37fc83441b16034566b
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
36864200e0eaf5284d884a0e77d31646
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00

POSSIBLE SECRETS
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

SCAN LOGS

Timestamp	Event	Error
2024-09-01 20:41:34	Generating Hashes	OK
2024-09-01 20:41:34	Extracting APK	OK
2024-09-01 20:41:34	Unzipping	OK
2024-09-01 20:41:36	Getting Hardcoded Certificates/Keystores	OK
2024-09-01 20:41:41	Parsing AndroidManifest.xml	OK
2024-09-01 20:41:41	Parsing APK with androguard	OK
2024-09-01 20:41:42	Extracting Manifest Data	OK

2024-09-01 20:41:42	Performing Static Analysis on: ClockWork (com.opsc7311.opsc7311poepart2)	OK
2024-09-01 20:41:42	Fetching Details from Play Store: com.opsc7311.opsc7311poepart2	OK
2024-09-01 20:41:43	Manifest Analysis Started	OK
2024-09-01 20:41:43	Checking for Malware Permissions	OK
2024-09-01 20:41:43	Fetching icon path	OK
2024-09-01 20:41:43	Library Binary Analysis Started	OK
2024-09-01 20:41:43	Reading Code Signing Certificate	OK
2024-09-01 20:41:43	Running APKiD 2.1.5	OK
2024-09-01 20:41:51	Updating Trackers Database....	OK
2024-09-01 20:41:51	Detecting Trackers	OK
2024-09-01 20:41:53	Decompiling APK to Java with jadx	OK

2024-09-01 20:42:49	Converting DEX to Smali	OK
2024-09-01 20:42:49	Code Analysis Started on - java_source	OK
2024-09-01 20:45:33	Android SAST Completed	OK
2024-09-01 20:45:33	Android API Analysis Started	OK
2024-09-01 20:48:06	Android Permission Mapping Started	OK
2024-09-01 20:48:16	Android Permission Mapping Completed	OK
2024-09-01 20:48:17	Finished Code Analysis, Email and URL Extraction	OK
2024-09-01 20:48:17	Extracting String data from APK	OK
2024-09-01 20:48:18	Extracting String data from Code	OK
2024-09-01 20:48:18	Extracting String values and entropies from Code	OK
2024-09-01 20:48:20	Performing Malware check on extracted domains	OK

2024-09-01 20:48:20	Saving to Database	OK

Report Generated by - MobSF v4.0.7

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.