MOBSF

ANDROID STATIC ANALYSIS REPORT

Drink Water Reminder (34.0)

File Name:	com.remind.drink.water.hourly_34.apk
Package Name:	com.remind.drink.water.hourly
Scan Date:	Sept. 1, 2025, 8:05 a.m.

App Security Score: 48/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	16	1	1	1

FILE INFORMATION

File Name: com.remind.drink.water.hourly_34.apk
Size: 5.13MB
MD5: 04e1dc3c9f6974dd5780014f5ef589e0
SHA1: 920d9c04517c8a89ccc7bdfdbb4f8032635e7286
SHA256: 81c2ac2feddf283df5e192fdbf50ab512445a846b2680de6b0568f2f30325e74

APP INFORMATION

App Name: Drink Water Reminder
Package Name: com.remind.drink.water.hourly
Main Activity: com.remind.drink.water.hourly.SplashActivity
Target SDK: 34
Min SDK: 19
Max SDK:
Android Version Name: 34.0
Android Version Code: 34

APP COMPONENTS

Activities: 18
Services: 10
Receivers: 13
Providers: 7
Exported Activities: 0
Exported Services: 1
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=84, ST=Hanoi, L=Hanoi, O=Healt ltd, OU=Water dept, CN=Hung Nguyen
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-08-23 01:19:15+00:00
Valid To: 2044-08-16 01:19:15+00:00
Issuer: C=84, ST=Hanoi, L=Hanoi, O=Healt ltd, OU=Water dept, CN=Hung Nguyen
Serial Number: 0x4e02474b
Hash Algorithm: sha256
md5: ad16e6c8a262d144d8108968bcd4bab2
sha1: 73262d5756e190be0da21d1467781dee31b00ce6

sha256: a4c4da099208aee58046831557e2c8a08f44347d0b015a6bb8e6de17791dd88c
sha512: 4d24c661ee7b7eb1999c9b491726bbe65110248a9042040f789132b5acf346d1ec71c85096af9aae0acfdaedfe32814001c738a7e98d2295965ee65c2601b0e6
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 4371782865e2adf3c168e0014918f25edec5ea829381e7f610f9f1d157ff7d16
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.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.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
com.android.alarm.permission.SET_ALARM	unknown	Unknown permission	Unknown permission from android reference
android.permission.EXPAND_STATUS_BAR	normal	expand/collapse status bar	Allows application to expand or collapse the status bar.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.READ_MEDIA_AUDIO	dangerous	allows reading audio files from external storage.	Allows an application to read audio files from external storage.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

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.
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.
android.permission.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check
	FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

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

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **5** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 4.4-4.4.4, [minSdk=19]	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	Broadcast Receiver (com.remind.drink.water.hourly.service.PermanentReceiver) 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.
3	Launch Mode of activity (com.google.android.gms.ads.NotificationHandlerActivity) 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	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
5	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.
6	High Intent Priority (999) - {1} Hit(s) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: **1** | WARNING: **8** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a/a.java a3/a.java a4/b.java a5/al1.java a5/ba.java a5/c9.java a5/ep1.java a5/gl.java a5/hg2.java a5/hn1.java a5/ic.java a5/k11.java a5/k50.java a5/md1.java a5/ml2.java a5/ql2.java a5/rd.java a5/s9.java a5/sn1.java a5/t4.java a5/td2.java a5/to1.java a5/uc.java a5/v30.java a5/xc.java a5/yc0.java a5/z51.java b0/k.java b4/g1.java b4/j.java b4/j1.java b4/k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b8/g.java b8/i.java b8/j.java c0/c.java c0/d.java c0/e.java c0/f.java c0/g.java c0/l.java c0/m.java c3/g.java c5/g.java com/remind/drink/water/hourly/MainActivity.java com/remind/drink/water/hourly/WaterApp.java com/remind/drink/water/hourly/notification/RemoteReceiver.java com/remind/drink/water/hourly/service/AlarmReceiver.java com/remind/drink/water/hourly/service/PermanentReceiver.java d0/a.java d0/m.java e1/g.java e1/h.java e2/c.java e2/d.java e2/e.java e2/i.java e2/q.java f/f.java f/i.java f/r.java f/t.java f3/b.java f5/g.java f5/g1.java f5/i.java f5/j1.java f5/l1.java f5/r.java f5/x.java g/a.java g0/h.java g5/a5.java g5/c2.java g5/g1.java g5/l0.java g5/n0.java g5/q4.java g5/v4.java g5/w4.java g5/y4.java g5/z4.java h1/c.java h2/a.java h2/b.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	h5/p.java h6/d.java i1/b.java i3/j.java j/g.java j0/b.java k0/a0.java k0/b.java k0/d1.java k0/f.java k0/r.java k0/u0.java k1/a.java k5/m2.java k5/m6.java k5/r5.java k5/x5.java l/c0.java l/e0.java l/h.java l/h0.java l/i.java l/n0.java l/r0.java l/t.java l/u0.java l/v.java l/y.java l1/t.java l1/u.java l1/v.java l1/w.java l1/x.java l1/y.java l2/d.java l3/a.java l6/j.java m1/h.java m7/u.java m9/c.java n0/i.java n9/a.java n9/c.java o0/b.java p1/h.java p4/c0.java p4/e.java p4/f.java p4/i.java p4/j.java p4/l.java p4/t.java p4/x.java p5/g.java q0/a.java q2/b0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				q2/b0.java q2/u.java q7/d.java r0/e.java r0/h.java r4/d.java r4/g0.java r4/i0.java r4/u.java r4/w.java r7/a.java s4/a1.java s4/b.java s4/e.java s4/h0.java s4/o.java s4/o0.java s4/s0.java s4/t.java s4/w.java s4/y0.java s7/g.java t2/a.java t2/b.java t5/a.java u/g.java u6/c.java v2/j.java v4/b.java w0/a.java w0/c.java w3/a.java w3/b.java w4/b.java w4/i.java w6/b.java w7/b.java x6/c.java y0/a.java z/f.java z3/e3.java z4/b.java
2	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	w0/c.java w6/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	a5/fh2.java a5/gy.java a5/hg2.java a5/ki2.java a5/uc.java a5/yc0.java a5/zn2.java d9/a.java d9/b.java e9/a.java g5/c2.java k5/e6.java m7/h.java m7/j.java z3/p.java
4	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	a5/t01.java a5/wz0.java com/remind/drink/water/hourly/database/alarm/dur.java i1/a.java k5/f2.java k5/k.java k5/l.java k5/l6.java k5/x5.java o3/d0.java o3/k.java o3/w.java s7/e.java t7/a.java x4/a.java
5	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	a5/g80.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	a5/jg.java a5/kc.java f5/g0.java k5/e6.java z3/p.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	a5/w12.java w6/b.java x6/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	a5/er1.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	a5/ep1.java l1/u.java
10	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	a5/gd.java
11	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	a5/fl.java a5/nk.java a5/zh.java q7/d.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	a5/aa.java a5/gn1.java a5/j0.java a5/o60.java a5/rd.java g1/a.java i1/b.java m2/c.java m2/d.java w0/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	a4/a.java a5/cr.java a5/d11.java a5/dr.java a5/fx.java a5/g80.java a5/gl.java a5/qb1.java a5/tz.java a5/u21.java a5/ul.java a5/w70.java a8/h.java a8/i.java com/lib/rate/RateDialogAct.java f5/x.java k5/l4.java k5/x5.java m7/u.java p4/f.java q7/d.java s7/g.java y3/m.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	a4/a.java a5/d11.java a5/dr.java a5/fx.java a5/u21.java a5/w70.java a8/i.java m7/u.java p4/f.java y3/m.java
00036	Get resource file from res/raw directory	reflection	a5/dr.java a5/g80.java a5/qb1.java l/h0.java p4/f.java
00096	Connect to a URL and set request method	command network	a5/g70.java a5/rd2.java a5/u9.java f3/b.java f5/n1.java m2/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	a5/g70.java a5/mz0.java a5/rd2.java a5/v60.java f3/b.java f5/n1.java k5/l4.java k5/q2.java m2/d.java x6/c.java
00109	Connect to a URL and get the response code	network command	a5/g70.java a5/mz0.java a5/on1.java a5/rd2.java a5/u9.java a5/v60.java a5/w70.java a5/y30.java f3/b.java f5/n1.java k5/l4.java k5/q2.java m2/d.java w3/b.java x6/c.java
00072	Write HTTP input stream into a file	command network file	a5/o60.java
00028	Read file from assets directory	file	a5/a02.java
00013	Read file and put it into a stream	file	a5/aa.java a5/rd.java a5/s22.java a5/ve2.java a5/x.java a5/ym1.java b4/u.java c0/e.java c0/f.java c0/m.java g1/b.java l1/u.java m2/c.java m2/d.java w6/c.java
00034	Query the current data network type	collection network	a5/tz.java b4/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	a5/g70.java a5/rd2.java a5/v60.java k5/q2.java m2/d.java
00094	Connect to a URL and read data from it	command network	a5/g70.java a5/mz0.java a5/rd2.java a5/u9.java a5/v60.java k5/l4.java k5/q2.java
00108	Read the input stream from given URL	network command	a5/g70.java a5/mz0.java a5/rd2.java a5/v60.java k5/l4.java k5/q2.java
00147	Get the time of current location	collection location	f/t.java
00075	Get location of the device	collection location	f/t.java
00115	Get last known location of the device	collection location	f/t.java
00091	Retrieve data from broadcast	collection	b4/s1.java com/remind/drink/water/hourly/MainActivity.java q2/y.java
00202	Make a phone call	control	a5/fx.java a5/w70.java
00203	Put a phone number into an intent	control	a5/fx.java a5/w70.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	h0/e.java t7/e.java
00191	Get messages in the SMS inbox	sms	l/h0.java s7/g.java
00003	Put the compressed bitmap data into JSON object	camera	a5/ev0.java b4/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00189	Get the content of a SMS message	sms	h0/e.java
00188	Get the address of a SMS message	sms	h0/e.java
00200	Query data from the contact list	collection contact	h0/e.java
00187	Query a URI and check the result	collection sms calllog calendar	h0/e.java
00201	Query data from the call log	collection calllog	h0/e.java
00012	Read data and put it into a buffer stream	file	a5/aa.java
00024	Write file after Base64 decoding	reflection file	a5/rd.java
00014	Read file into a stream and put it into a JSON object	file	b4/u.java w6/c.java
00046	Method reflection	reflection	c7/o.java
00056	Modify voice volume	control	w7/b.java
00125	Check if the given file path exist	file	q7/d.java
00153	Send binary data over HTTP	http	a5/u9.java
00132	Query The ISO country code	telephony collection	a5/wp2.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	4/44	android.permission.FOREGROUND_SERVICE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, com.google.android.gms.permission.AD_ID, 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
www.googleadservices.com	ok	**IP:** 142.250.74.2 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
support.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
googleads.g.doubleclick.net	ok	**IP:** 216.58.211.2 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
fundingchoicesmessages.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
googlemobileadssdk.page.link	ok	**IP:** 142.250.74.129 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.74.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sites.google.com	ok	**IP:** 216.58.207.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 142.250.74.68 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
csi.gstatic.com	ok	**IP:** 216.239.32.3 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app-measurement.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 216.58.207.194 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.example.com	ok	**IP:** 23.220.73.43 **Country:** Colombia **Region:** Antioquia **City:** Medellin **Latitude:** 6.251840 **Longitude:** -75.563591 **View:** Google Map
admob-gmats.uc.r.appspot.com	ok	**IP:** 142.250.74.20 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
imasdk.googleapis.com	ok	**IP:** 142.250.74.170 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ns.adobe.com	ok	No Geolocation information available.
schemas.android.com	ok	No Geolocation information available.
google.com	ok	**IP:** 216.58.207.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developers.google.com	ok	**IP:** 172.217.21.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gl	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
waterreminder.qa@gmail.com	m7/u.java
u0013android@android.com0 u0013android@android.com	p4/s.java

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
9mv9Ihk+HIE8P3WJWSjhrxWrdB7cEu1gaxdteA5kBJ6DKumpWYk1Q5Vf8aocVg4i
gL88T2vBvJS+jBemUvhPpVS5IeaU7cU4wFVgyT6PJl7pFldWXOd3mZxVZIQUSll5
Jz2tk/JKeGJKcc4wwXH5Pf6ZM64fYgV4wWxByPOgNQE=
s1ejGoWFNJedDDJqGqL3B22F5ZMvy0oaymBcWJepS9Hv4/6KtsHBpmbtFfwgqqen
I5l5b06e/m6OPcJVryww5aceHDWuWNMRDm4mYVrBvJQ=
NOrE2caDXO4nkFR2Fjy7NgGPKtPlIg1WAorknI/US68=
Q+fOnDUQnIPH75lusFutOgWOI4DeJ6z7X13oo1pZ5m19Kfyi56UOJglWSBqO3AzA
49f946663a8deb7054212b8adda248c6
aC7c3pDenGsdb0eFildzKOBrhobw8fKkmd52rTlBEKM=
sK9i540XcONymgaiZVMKYXr1VbNcwMhjwo2LFhhSCFg=
1ZhioNexfONxLbr8oNixHPTbX/qv3RsJiyYoeeb0m+g=
8UC+BMIoCN+KAKrN9TZmuJsGMmo3RUHS+FjVMSp9QfgjxjGZ10kqO/oSdOn5Rw29
qUEdP6yfmpdCkPVqoE8EyrX/MPjGh4YKRo5g3kOeMoc=
A3EfeXObjqx38Tdc4wdTZSQNpfpw6YVck+944M4A/m0=
tfuuP59pzWN+H8zv1geT3jADiBKBGMQRjmCPoIvL5f45Lvl5qgJ0PgBqZF4WPnQj
7qOZVP58PfP3kLkbSBo98onihlohkIEpZC40FvE5nnCJ8ryn0NERK9JAnlww55zq

POSSIBLE SECRETS
1OxyLDHu2cwu0U7XKtDO3q+DghLeQ8xcTgpGCDWDuEeCcfs+HPxSt8kldIfiq1K0
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e2056696577731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e0603550403130 7416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e2056696577731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e0603550403130 7416e64726f69643082012030 0d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e2056696577731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e0603550403130 7416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d01010405000382010100 6dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
Ee4p/yPQz67p3LoSNbpt1G8K9rDuoWxBYT8E4CbWyr8=
bObXLZFRWAdU6+me08AeNX2ciqxi45ddv3QSqAplzos=
RSyr2AK130nKbepDTsaNV0Uv17TWUb4O6ebIiV3GgVs=
MIrDuKB7N0O22daoYjLtFOJg5TtVRHK1+0ktwmGNtdU=
SMfJnKfhfLLyTw7dzHC+3CXVRNFLWK4N2mQHKB3gm/o=
nIX5dAPvXYWFIvHlyxyLt0TnZ91UnAjFxZwf2qcoWSGcs+p5B5p88VCOzepPfMpE
B3EEABB8EE11C2BE770B684D95219ECB
s7rU1m4XsqJ83s2reIjdkboWJYkg+gYouDrDcn3Ghpw=
zahwJ4oRFMB+Gn9BGkfZDZ8TzDEfKTB8Y6I4bT4vlwkVFXvqlnkWd7htbiUzWQyR
gzR6fJL0MpYPfJ/UkFL9UHjS7jlytQ+eyVRsQJTsxzK4yqDaskM4UtldyBDUp+Z9
1eWk7vHD3Ee+FybzKEoWLH07Pvdxo5flYR768ntLvpJZNSFjE7xgNzi+al9tiZC4
Y0trGqGVEUAa7A3LYgSQFKe4N9h1BuTC7OKFYCHfLSg=
xLOAO7msIR4UFUyldUn5stL2wwbLdISu2CSlTLg4f6Q=
3PwoDnm3HnsskB+3ZnJHoZ7BzV0InxUqaAwJBlSwKFs=
ttuIHg/yfWDxJlotLoMLf9WBnVTbWFFKY03C8KHR8FAhIQHccw4LaDLJatYkpo23

POSSIBLE SECRETS
BkxOKZDOMH8NUFJEmpCq1X+PtIP0kLI1Ua0ujwsrkUE=
ZVHCdOeJUA1S4bCrFb9VMsUCP8Sf65wDnbBE+q4M36k=
XCj6cS5OVeEeObzd394PGDbjTuQh+vSye2UT6221ugsKtO2/oznWOSes2cnebrVR
ZHFOx+FjaOsuI7gEkIcfA8auDnyRWXmT0qbiHVEO6U1RLulNSOFK3tPEgm+pvQxr
c103703e120ae8cc73c9248622f3cd1e
Eg2eC3eNesWzbAUlNzxj1mXRcYgmzS654CxZFoVQbAM=
MbAcGuLi+XGl3MsgqAiQYLikemL120ZFxn+dIhaD+rHWJuTeO/M8+1c58cczHjCs
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d01010405003081943l0b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930313233333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d01010405000382010100019d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
w5tjCRfZfXWJzckDvIkXwf5aGJEVejLzfxhnwyqJH5E=
zmLnsak1Fo/LHy30EeWswBCxcOoFKuH08l3DkSTUgzb476o6nl+C8ZUC+d8tLJwZ
y+BEEb1lYOUGwTehZ9Vlg/2gibmtEOjDZzKXHhs5BV0=
beFEMZ/YBSUug4MSXb2BKymKiM6ZxOOlxExWa37jMlM=
fxU2A2MjpZ4aJWGzXeMNURilSCaKosw3oXImrqnhSVmXB+tMi32JakdNlHCV3t0c
KHu8Xbxzr2mu9S25CNgKE5zXBf18Zj2waiAPYoFRjyhOXCyg+mYLv2x/JjCH7GjX
hMVcCX1S6+m7rVEDNdCHhVgXRFILMOQ9RgLSmTdPHeNgAU8CbmBsymKBuqLQcQaU
iibTgWRTbrwM2W7HZGJP5cjM0DLiCyA9TVVy1genRaa4nvgE3+CiRN/Fx87DVDsO

POSSIBLE SECRETS
r6m9xWOlfK6iHuNH3QiJQf71aQCKDM6NhABQId+yaKg=

PLAYSTORE INFORMATION

Title: Water Reminder - Remind Drink

Score: 4.8311305 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.remind.drink.water.hourly

Developer Details: recorder & smart apps, 5961211893873529920, None, https://www.smartapp-ogs.com, olympic.game.studio@gmail.com,

Release Date: Oct 10, 2019 **Privacy Policy:** Privacy link

Description:

Reminds you to drink water, a great application that take care of your health. Let drink water remind you to drink water if you always forget it. The best healthcare application for you. And it's totally free. If you're too busy to remember having to drink enough and regularly, don't worry, there's "drink water" to help you solve that problem. Drink water reminder is an application with main function is to help us keep water tracker we need to replenish and water drinking reminder in time. Users only need to select a gender and enter a weight number, it will help you calculate how much water should you drink per day. You can also tracker water history, reach your daily goal to open the respective achievements, and many other useful functions, ... Water drinking reminder will help you build a good habit with healthy body. * Main features : - Easy to use, beautiful interface. - Based on gender, weight will let you know how much water should drink a day. - Human body graphics to drinking water tracker - Diverse menu of nearly 20 different drinks. - Can choose the amount of water each time. - Smart reminder: time mode go to bed so you don't get drink water reminder. - Water tracker by week, month and year in the chart - Can adjust the amount of drinking water in the past. - Can option interval time receive drink water reminder message - Achievements to encourage you to accomplish your daily goal. - Allows integration of data into health application. With many benefits of drinking water such as weight loss, healthy skin, reduced fatigue and preventing many diseases, ... an drink water reminder application is extremely useful and necessary. So, "drink water" is like a companion to your health. Use now to your water tracker. If you want to keep healthy, drink enough. Want to drink enough, install water drinking reminder ! If you feel this water drinking reminder application is useful, share it with your friends and family. Above all, we are excited and hope to receive your feedback or ideas for we can complete and develop this app in the next version.Any feedback please send to my email

SCAN LOGS

Timestamp	Event	Error
2025-09-01 08:05:31	Generating Hashes	OK
2025-09-01 08:05:31	Extracting APK	OK
2025-09-01 08:05:31	Unzipping	OK
2025-09-01 08:05:32	Parsing APK with androguard	OK
2025-09-01 08:05:33	Extracting APK features using aapt/aapt2	OK

2025-09-01 08:05:33	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 08:05:35	Parsing AndroidManifest.xml	OK
2025-09-01 08:05:35	Extracting Manifest Data	OK
2025-09-01 08:05:35	Manifest Analysis Started	OK
2025-09-01 08:05:35	Performing Static Analysis on: Drink Water Reminder (com.remind.drink.water.hourly)	OK
2025-09-01 08:05:37	Fetching Details from Play Store: com.remind.drink.water.hourly	OK
2025-09-01 08:05:38	Checking for Malware Permissions	OK
2025-09-01 08:05:38	Fetching icon path	OK
2025-09-01 08:05:38	Library Binary Analysis Started	OK
2025-09-01 08:05:38	Reading Code Signing Certificate	OK
2025-09-01 08:05:39	Running APKiD 2.1.5	OK
2025-09-01 08:05:42	Detecting Trackers	OK
2025-09-01 08:05:43	Decompiling APK to Java with JADX	OK
2025-09-01 08:05:53	Converting DEX to Smali	OK
2025-09-01 08:05:53	Code Analysis Started on - java_source	OK

2025-09-01 08:05:55	Android SBOM Analysis Completed	OK
2025-09-01 08:06:02	Android SAST Completed	OK
2025-09-01 08:06:02	Android API Analysis Started	OK
2025-09-01 08:06:10	Android API Analysis Completed	OK
2025-09-01 08:06:11	Android Permission Mapping Started	OK
2025-09-01 08:06:17	Android Permission Mapping Completed	OK
2025-09-01 08:06:17	Android Behaviour Analysis Started	OK
2025-09-01 08:06:27	Android Behaviour Analysis Completed	OK
2025-09-01 08:06:27	Extracting Emails and URLs from Source Code	OK
2025-09-01 08:06:29	Email and URL Extraction Completed	OK
2025-09-01 08:06:29	Extracting String data from APK	OK
2025-09-01 08:06:29	Extracting String data from Code	OK
2025-09-01 08:06:29	Extracting String values and entropies from Code	OK
2025-09-01 08:06:30	Performing Malware check on extracted domains	OK
2025-09-01 08:06:32	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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.