ANDROID STATIC ANALYSIS REPORT

WWChildApp (1.1.87)

File Name:	WWChild (1).apk
Package Name:	com.awti.slc
Scan Date:	Aug. 10, 2024, 7:40 p.m.

App Security Score:	48/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	ℹ INFO	✓ SECURE	HOTSPOT
2	23	1	1	1

FILE INFORMATION

File Name: WWChild (1).apk
Size: 1.65MB
MD5: f61f9a58d2c46c2679e3584a9d816f34
SHA1: 70c33a61d5e196e9e18f2111827c1e52d136137e
SHA256: 1a358efae67f0c235cf1d6121acd7c65d3194e096b7d7136584d2df4028306a7

APP INFORMATION

App Name: WWChildApp
Package Name: com.awti.slc
Main Activity: com.awti.slc.installer.MainActivity
Target SDK: 30
Min SDK: 19
Max SDK:
Android Version Name: 1.1.87
Android Version Code: 121

APP COMPONENTS

Activities: 15
Services: 15
Receivers: 21
Providers: 1
Exported Activities: 0
Exported Services: 2
Exported Receivers: 11
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=US, ST=Connecticut, L=Westport, O=Awareness Technologies Inc, OU=Software Development, CN=Steven Schonberg
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-10-27 17:20:10+00:00
Valid To: 2067-10-15 17:20:10+00:00
Issuer: C=US, ST=Connecticut, L=Westport, O=Awareness Technologies Inc, OU=Software Development, CN=Steven Schonberg
Serial Number: 0x12b4b032
Hash Algorithm: sha256
md5: 18dece708c8f55fc70bf7f0464c2b555
sha1: b9d5baedcf0c711317e8b6e54d60f0a5edee9517

```
sha256: 78754d29f4913953391d65044060b044a6f7bccd863d81c665d3823f8781094c
sha512: 465fb07546f048c05937bebd556201d232e6a71895446b6173b913c6e7d63eb6c520618b3eaf5413275729d741ed9240bbd6055677140442dd29dad2113c0bee
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 6ba212b9cae1464207645c27888f048159345949d0d78669646d4a4a86fc75af
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.READ_PRIVILEGED_PHONE_STATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.RECEIVE_WAP_PUSH	dangerous	receive WAP	Allows application to receive and process WAP messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.RECEIVE_MMS	dangerous	receive MMS	Allows application to receive and process MMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
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.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.RAISED_THREAD_PRIORITY	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
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.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_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
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.READ_CALL_LOG	dangerous	grants read access to the user's call log.	Allows an application to read the user's call log.
android.permission.PROCESS_OUTGOING_CALLS	dangerous	intercept outgoing calls	Allows application to process outgoing calls and change the number to be dialled. Malicious applications may monitor, redirect or prevent outgoing calls.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.android.browser.permission.READ_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference
com.android.browser.permission.WRITE_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.GET_TOP_ACTIVITY_INF0	unknown	Unknown permission	Unknown permission from android reference
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.KILL_BACKGROUND_PROCESSES	normal	kill background processes	Allows an application to kill background processes of other applications, even if memory is not low.
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.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
android.permission.INTERACT_ACROSS_USERS	unknown	Unknown permission	Unknown permission from android reference
android.permission.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
android.permission.BIND_ACCESSIBILITY_SERVICE	signature	required by AccessibilityServices for system binding.	Must be required by an AccessibilityService, to ensure that only the system can bind to it.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

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: **15** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched 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	Launch Mode of activity (com.awti.slc.installer.MainActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
3	Launch Mode of activity (com.awti.slc.installer.LoginActivity) 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 (com.awti.slc.client.WWFObserverService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_ACCESSIBILITY_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.
5	Broadcast Receiver (com.awti.slc.client.BootBroadcastReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
6	Broadcast Receiver (com.awti.slc.client.ShutdownBroadcastReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
7	Broadcast Receiver (com.awti.slc.client.StillRunningBroadcastReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
8	Broadcast Receiver (com.awti.slc.client.PackageAddedReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
9	Broadcast Receiver (com.awti.slc.client.UninstallProtectionReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_DEVICE_ADMIN [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.

NO	ISSUE	SEVERITY	DESCRIPTION
10	Broadcast Receiver (com.awti.slc.client.SMSBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BROADCAST_SMS [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.
11	Broadcast Receiver (com.awti.slc.client.MediaStatusBroadcastReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
12	Broadcast Receiver (com.awti.slc.client.AppMonitorBroadcastReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
13	Broadcast Receiver (com.awti.slc.client.ScreenshotReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
14	Broadcast Receiver (com.awti.slc.client.MessageHandler) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
15	Service (com.awti.messaging.MessagingService) is not Protected. An intent-filter exists.	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.
16	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.

CODE ANALYSIS

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

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	b/c/c/a.java b/c/e/b.java b/c/f/b.java b/c/f/c.java b/d/a/a.java b/e/a/a.java b/e/a/b.java b/e/a/e.java b/e/a/j.java b/e/a/m.java b/f/a/a.java b/g/a/b.java c/b/a/a/i/y/a.java c/b/a/b/a/a/a.java c/b/a/b/a/a/d.java c/b/a/b/c/a0.java c/b/a/b/c/b.java c/b/a/b/c/d.java c/b/a/b/c/h.java c/b/a/b/c/r.java c/b/a/b/c/s.java c/b/a/b/c/u.java c/b/a/b/c/x.java c/b/a/b/c/y.java c/b/a/b/e/e/b1.java c/b/a/b/e/e/e6.java c/b/a/b/e/e/f6.java c/b/a/b/e/e/j6.java c/b/a/b/e/e/k6.java c/b/a/b/e/e/l6.java c/b/a/b/e/e/q6.java c/b/a/b/e/e/u1.java c/b/a/b/e/e/v0.java c/b/a/b/e/e/w2.java c/b/a/b/e/e/w5.java c/b/a/b/f/b/a.java c/b/a/b/g/a.java c/c/a/a/a.java com/awti/slc/client/ScOverlayActivity.java com/awti/slc/client/c0.java com/awti/slc/client/f0/a.java com/awti/slc/client/o.java com/awti/slc/client/p.java com/awti/slc/common/Globals.java com/awti/slc/installer/m.java
2	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/awti/slc/common/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	c/b/a/a/i/a0/j/a0.java c/b/a/a/i/a0/j/r0.java c/b/a/a/i/a0/j/t0.java com/awti/slc/client/i.java
4	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/awti/slc/client/ScOverlayActivity.java com/awti/slc/common/i.java com/awti/slc/common/j.java
5	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	com/awti/slc/common/i.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	c/b/a/b/e/e/w2.java
7	The App uses ECB mode in Cryptographic encryption algorithm. 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	com/awti/slc/client/l.java
8	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	c/b/a/b/e/e/q6.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	17/24	android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.READ_SMS, android.permission.RECEIVE_SMS, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.READ_PHONE_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_FINE_LOCATION, android.permission.GET_TASKS, android.permission.READ_CONTACTS, android.permission.READ_CALL_LOG, android.permission.ACCESS_NETWORK_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.VIBRATE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.READ_EXTERNAL_STORAGE

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	9/45	android.permission.CHANGE_WIFI_STATE, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.PROCESS_OUTGOING_CALLS, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.FOREGROUND_SERVICE, android.permission.PACKAGE_USAGE_STATS, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID

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
data.sonarcentral.com	ok	**IP:** 104.26.1.164 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
awareness.wifi	ok	No Geolocation information available.
login.webwatcher.com	ok	**IP:** 172.67.7.195 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
datatest.webwatcherdata.com	ok	**IP:** 104.26.11.55 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.webwatcher.com	ok	**IP:** 141.193.213.20 **Country:** United States of America **Region:** Texas **City:** Austin **Latitude:** 30.271158 **Longitude:** -97.741699 **View:** Google Map
goo.gl	ok	**IP:** 172.217.19.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
data.webwatcherdata.com	ok	**IP:** 104.26.10.55 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
webwatcher-child-app.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
www.youtube.com	ok	**IP:** 142.250.180.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	**IP:** 142.250.201.196 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app-measurement.com	ok	**IP:** 142.251.208.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.rcomlogin.com	ok	**IP:** 97.77.62.75 **Country:** United States of America **Region:** Texas **City:** Plano **Latitude:** 33.019840 **Longitude:** -96.698891 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
api.awarenesstechnologies.com	ok	**IP:** 172.67.15.147 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
test.webwatcher.com	ok	No Geolocation information available.
datademo.webwatcherdata.com	ok	**IP:** 172.67.74.177 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
pagead2.googlesyndication.com	ok	**IP:** 142.251.39.2 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://webwatcher-child-app.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://webwatcher-child-app.firebaseio.com"
"google_api_key" : "AIzaSyAy-eHpHEh0ShIQ6Hbh_z-KGBfNfjakqCw"
"google_crash_reporting_api_key" : "AIzaSyAy-eHpHEh0ShIQ6Hbh_z-KGBfNfjakqCw"
"password" : "Password"

POSSIBLE SECRETS
470fa2b4ae81cd56ecbcda9735803434cec591fa

SCAN LOGS

Timestamp	Event	Error
2024-08-10 19:40:52	Generating Hashes	OK
2024-08-10 19:40:52	Extracting APK	OK
2024-08-10 19:40:52	Unzipping	OK
2024-08-10 19:40:52	Getting Hardcoded Certificates/Keystores	OK
2024-08-10 19:40:53	Parsing AndroidManifest.xml	OK
2024-08-10 19:40:53	Parsing APK with androguard	OK
2024-08-10 19:40:53	Extracting Manifest Data	OK
2024-08-10 19:40:53	Performing Static Analysis on: WWChildApp (com.awti.slc)	OK
2024-08-10 19:40:53	Fetching Details from Play Store: com.awti.slc	OK
2024-08-10 19:40:54	Manifest Analysis Started	OK
2024-08-10 19:40:54	Checking for Malware Permissions	OK

2024-08-10 19:40:54	Fetching icon path	OK
2024-08-10 19:40:54	Library Binary Analysis Started	OK
2024-08-10 19:40:54	Reading Code Signing Certificate	OK
2024-08-10 19:40:54	Running APKiD 2.1.5	OK
2024-08-10 19:40:56	Detecting Trackers	OK
2024-08-10 19:40:56	Decompiling APK to Java with jadx	OK
2024-08-10 19:41:01	Converting DEX to Smali	OK
2024-08-10 19:41:01	Code Analysis Started on - java_source	OK
2024-08-10 19:41:04	Android SAST Completed	OK
2024-08-10 19:41:04	Android API Analysis Started	OK
2024-08-10 19:41:07	Android Permission Mapping Started	OK
2024-08-10 19:41:18	Android Permission Mapping Completed	OK
2024-08-10 19:41:19	Finished Code Analysis, Email and URL Extraction	OK
2024-08-10 19:41:19	Extracting String data from APK	OK
2024-08-10 19:41:19	Extracting String data from Code	OK

2024-08-10 19:41:19	Extracting String values and entropies from Code	OK
2024-08-10 19:41:20	Performing Malware check on extracted domains	OK
2024-08-10 19:41:24	Saving to Database	OK

Report Generated by - MobSF v4.0.6

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.