MOBSF

ANDROID STATIC ANALYSIS REPORT

MaxView Jobs (2024.5.10)

File Name:	com.maximstaffing.app_1606.apk
Package Name:	com.maximstaffing.app
Scan Date:	Aug. 31, 2025, 2:32 a.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	17	3	2	1

FILE INFORMATION

File Name: com.maximstaffing.app_1606.apk
Size: 17.32MB
MD5: 4e57123729d77c53f2685dc17ffa79d4
SHA1: 988f53a3755a90012330171768395a3ca673abcb
SHA256: 056c38d0a1a525cd0a09b6a3f3723c88e5e82960928c177e2f9df0ff6a659f32

APP INFORMATION

App Name: MaxView Jobs
Package Name: com.maximstaffing.app
Main Activity: com.maximstaffing.app.MainActivity
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 2024.5.10

Android Version Code: 1606

APP COMPONENTS

Activities: 5
Services: 15
Receivers: 13
Providers: 5
Exported Activities: 0
Exported Services: 2
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-06-17 10:55:36+00:00
Valid To: 2052-06-17 10:55:36+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xd48aad0b2801954600dd086fbe38e211edc5e866
Hash Algorithm: sha256
md5: a4b75a26fc614d77bac2d70409808549
sha1: 87a747126e74a948067ddac2e295c788b841e974
sha256: 887111837abcc07573d39528c83f3c4c1ac11d97adfac4d3fdd95816036f1e2d
sha512: 98fe292440af5c3df1d0abd88c95db5aa67c2fdac9966f1569292371c40d4a7f2f46e37b0dece5ac43fbb3540c73bdbecd06a708236013a12b8be24488209669
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 3a533a97e3de1c7807defa7a2b674d820ccc7b88393ca0dd81fecd6ffd731717
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_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
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.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.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.
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_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.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.maximstaffing.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
4e57123729d77c53f2685dc17ffa79d4.apk	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>possible VM check</td></tr></table>
classes.dex	<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 possible Build.SERIAL 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>r8 without marker (suspicious)</td></tr></table>

FILE	DETAILS
classes2.dex	<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 possible Build.SERIAL check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.maximstaffing.app.MainActivity	Schemes: com.maximstaffing.app://, exp+maxim://,

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: 6 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Broadcast Receiver (io.invertase.firebase.messaging.ReactNativeFirebaseMessagingReceiver) 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.
4	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.
5	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
6	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.
7	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.

</> CODE ANALYSIS

HIGH: **0** | WARNING: **7** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a1/n.java a2/a.java b0/e.java b2/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b2/b.java b3/a.java c2/d.java c2/e.java c4/f.java cb/g.java cc/l.java ch/i.java com/bumptech/glide/b.java com/reactnativecommunity/asyncstorage/h.java com/rnmaps/maps/MapTileWorker.java com/rnmaps/maps/i.java com/rnmaps/maps/p.java com/rnmaps/maps/q.java com/rnmaps/maps/s.java com/swmansion/gesturehandler/react/RNGestureHandlerModule.java com/swmansion/gesturehandler/react/i.java com/swmansion/gesturehandler/react/j.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/th3rdwave/safeareacontext/l.java e0/c.java e2/b.java e2/j.java e2/l.java e8/a.java e8/d.java eg/a.java expo/modules/notifications/service/NotificationsService.java f2/c.java f2/e.java fb/s.java fg/a.java fg/b.java g1/c.java g2/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				g2/i.java g2/k.java g2/q.java g2/z.java ga/d.java gh/a.java h2/i.java h2/k.java ha/b.java hc/h2.java hd/a.java hd/e.java hf/e.java i2/e.java i2/i.java i8/g.java io/invertase/firebase/app/ReactNativeFirebaseAppModule.java io/invertase/firebase/app/a.java io/invertase/firebase/crashlytics/ReactNativeFirebaseCrashlyticsInitProvider.java io/invertase/firebase/crashlytics/ReactNativeFirebaseCrashlyticsModule.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingModule.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingReceiver.java io/invertase/firebase/perf/i.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java j2/a.java j9/f.java ja/g.java k0/b.java k0/d.java k1/a.java k2/c.java k2/d.java k2/f.java k2/r.java k2/s.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	k8/a0.java k8/b.java k8/b0.java k8/c.java k8/j.java k8/t.java k8/v.java k8/x.java k9/q0.java kd/f0.java kd/h.java kd/i0.java kd/l.java kd/l0.java kd/z.java ke/b.java km/c.java l1/m0.java l8/c0.java l8/g0.java l8/j.java l8/l0.java l8/o.java l8/p.java l8/q0.java l8/t.java l9/e.java ld/a.java m2/m.java md/c.java md/f.java n1/j.java n2/c.java n2/e.java n2/f0.java n2/j.java n2/q.java n2/r.java n2/u.java n8/c0.java o8/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o8/c.java o8/c0.java o8/c1.java o8/d1.java o8/e1.java o8/f0.java o8/g1.java o8/m1.java o8/q1.java o8/z0.java o9/a.java oc/b.java oe/b.java oe/d.java om/c.java p0/a.java pc/c.java q5/f.java q5/l.java q9/a.java qh/g.java qh/m.java r0/c.java r2/a.java r2/d.java r2/j.java r8/a.java r9/a.java s7/k.java s8/b.java sg/b.java sg/d.java sg/e.java t0/a.java t2/e.java t2/f.java t2/k.java t2/l.java t2/n.java t2/o.java t8/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				t8/o.java t8/p.java u2/d.java u9/c.java ua/f.java uc/e.java ud/i.java ue/e.java v/f.java v4/d.java v7/a.java w0/c.java w2/h.java w8/h.java wd/f.java wd/n.java wd/p.java wg/a.java x8/d.java xc/c.java xg/c.java xg/d.java xg/f.java ym/e.java za/g.java za/o.java ze/n.java
2	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	ag/b.java jc/z.java oc/b.java r3/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	d2/g.java expo/modules/adapters/react/NativeModulesProxy.java expo/modules/webbrowser/OpenBrowserOptions.java g2/d.java g2/p.java g2/x.java g5/h.java gb/b.java hb/e.java hb/w.java io/grpc/internal/p2.java jd/b.java lc/b.java
4	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	bn/d.java bn/h.java cd/d.java ij/a.java ij/b.java io/grpc/internal/e0.java io/grpc/internal/g0.java io/grpc/internal/r1.java io/grpc/internal/z1.java jf/b.java jh/i.java jj/a.java nm/z.java ph/f.java ph/i.java wd/o.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	com/rnmaps/maps/MapModule.java com/rnmaps/maps/a.java e3/a.java oc/c.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	s6/a.java
7	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/reactnativecommunity/asyncstorage/k.java h1/a.java z7/m0.java z7/t0.java
8	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	ch/i.java jf/c.java le/c.java oe/d.java xg/i.java
9	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	e3/a.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java o3/a.java
10	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	xm/d.java xm/e.java xm/j.java xm/k.java
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	fb/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	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	ye/a.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	ac/b.java expo/modules/notifications/service/NotificationsService.java hh/b.java hh/k.java l8/k.java le/c.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java ze/n.java
00091	Retrieve data from broadcast	collection	expo/modules/notifications/service/NotificationsService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/rnmaps/maps/d.java com/rnmaps/maps/l.java expo/modules/notifications/service/NotificationsService.java j7/a.java l8/k.java le/c.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java ze/n.java
00013	Read file and put it into a stream	file	b2/b.java c3/b.java cj/d.java cn/r.java com/bumptech/glide/load/a.java com/reactnativecommunity/asyncstorage/h.java com/rnmaps/maps/a.java com/rnmaps/maps/k.java com/rnmaps/maps/p.java e1/c.java fb/b0.java g0/m.java gb/f.java hc/q2.java hn/c.java k2/f.java kb/e.java mb/a.java oc/c.java ue/g.java ze/n.java
00187	Query a URI and check the result	collection sms calllog calendar	k0/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	f2/c.java k0/b.java k0/d.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/rnmaps/maps/p.java
00022	Open a file from given absolute path of the file	file	e1/a.java e3/f.java g0/m.java gb/f.java h1/b.java i3/c.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java o3/a.java wf/k0.java ze/n.java
00014	Read file into a stream and put it into a JSON object	file	gb/f.java mb/a.java oc/c.java
00109	Connect to a URL and get the response code	network command	e2/j.java e8/d.java i8/f.java pc/c.java wd/n.java
00162	Create InetSocketAddress object and connecting to it	socket	xm/c.java xm/k.java
00163	Create new Socket and connecting to it	socket	xm/c.java xm/k.java

RULE ID	BEHAVIOUR	LABEL	FILES
00114	Create a secure socket connection to the proxy address	network command	sm/f.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/a.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	hh/b.java hh/k.java l8/k.java le/c.java
00005	Get absolute path of file and put it to JSON object	file	gb/f.java
00094	Connect to a URL and read data from it	command network	jb/a.java l9/i0.java
00026	Method reflection	reflection	ak/a.java ak/b.java
00189	Get the content of a SMS message	sms	r3/f.java
00188	Get the address of a SMS message	sms	r3/f.java
00200	Query data from the contact list	collection contact	r3/f.java
00201	Query data from the call log	collection calllog	r3/f.java
00096	Connect to a URL and set request method	command network	pc/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	e2/j.java pc/c.java wd/n.java
00030	Connect to the remote server through the given URL	network	e2/j.java
00121	Create a directory	file command	ze/n.java
00024	Write file after Base64 decoding	reflection file	ze/n.java
00012	Read data and put it into a buffer stream	file	ze/n.java
00125	Check if the given file path exist	file	ze/n.java
00104	Check if the given path is directory	file	ze/n.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/122059485063/namespaces/firebase:fetch?key=AIzaSyDQBXRxEJRcjT0XeywEBJ7qnp6fV5sTs4c is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'DELETE_ACCOUNT': 'true', 'FACILITIES_DETAILS': 'true', 'FACILITIES_FILTER': 'false', 'FACILITIES_SORT': 'false', 'JOBS_COUNT': 'false', 'JOB_ALERT': 'true', 'JOB_ALERTS_EMAIL_NOTIFICATION': 'false', 'JOB_ALERTS_IMMEDIATELY': 'false', 'MAX_JOB_ALERTS': '10'}, 'state': 'UPDATE', 'templateVersion': '19'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.VIBRATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	3/44	com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_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
firebase.google.com	ok	**IP:** 142.250.176.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
expo.dev	ok	**IP:** 104.18.4.104 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
accounts.google.com	ok	**IP:** 142.250.101.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 142.250.176.3 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
issuetracker.google.com	ok	**IP:** 142.251.40.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.217.130 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
console.firebase.google.com	ok	**IP:** 142.250.217.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	l8/b0.java

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
"com.google.firebase.crashlytics.mapping_file_id" : "0b29fe4e7490428d86c5fc46d3a8262a"
"google_api_key" : "AIzaSyDQBXRxEJRcjT0XeywEBJ7qnp6fV5sTs4c"
"google_crash_reporting_api_key" : "AIzaSyDQBXRxEJRcjT0XeywEBJ7qnp6fV5sTs4c"
c103703e120ae8cc73c9248622f3cd1e

POSSIBLE SECRETS
49f946663a8deb7054212b8adda248c6
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa

PLAYSTORE INFORMATION

Title: MaxView Jobs by Amergis

Score: 3.4473684 **Installs:** 10,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.maximstaffing.app

Developer Details: Amergis Healthcare Staffing, Inc., Amergis+Healthcare+Staffing,+Inc., None, https://www.amergis.com/contact/, mobileapplicationsupport@amergis.com,

Release Date: May 11, 2023 **Privacy Policy:** Privacy link

Description:

MaxView Jobs is your one stop app for finding your next contract, or picking up a last minute shift. Through our new app, you can also track your application, complete onboarding, and track your hours and payments. With thousands of jobs nationwide in the healthcare, schools, and state and local settings, we offer you the flexibility that fits your lifestyle and career goals. Download the app today to get started! One-click apply Click apply on an open position and a recruiter will contact you with assignment details. Simplified onboarding Our credentialing team will be with you through every step so you’re ready to go to work. Track your progress The app lets your see where you’re at in the hiring process and can send you notifications for upcoming deadlines. Everything all in one place Submit your timecard, review paystubs, and quickly get in touch with your recruiter without leaving the app.

SCAN LOGS

Timestamp	Event	Error

2025-08-31 02:32:10	Generating Hashes	OK
2025-08-31 02:32:10	Extracting APK	OK
2025-08-31 02:32:10	Unzipping	OK
2025-08-31 02:32:12	Parsing APK with androguard	OK
2025-08-31 02:32:18	Extracting APK features using aapt/aapt2	OK
2025-08-31 02:32:18	Getting Hardcoded Certificates/Keystores	OK
2025-08-31 02:32:23	Parsing AndroidManifest.xml	OK
2025-08-31 02:32:23	Extracting Manifest Data	OK
2025-08-31 02:32:23	Manifest Analysis Started	OK
2025-08-31 02:32:23	Performing Static Analysis on: MaxView Jobs (com.maximstaffing.app)	OK
2025-08-31 02:32:24	Fetching Details from Play Store: com.maximstaffing.app	OK

2025-08-31 02:32:25	Checking for Malware Permissions	OK
2025-08-31 02:32:25	Fetching icon path	OK
2025-08-31 02:32:25	Library Binary Analysis Started	OK
2025-08-31 02:32:25	Reading Code Signing Certificate	OK
2025-08-31 02:32:30	Running APKiD 2.1.5	OK
2025-08-31 02:32:36	Detecting Trackers	OK
2025-08-31 02:32:49	Decompiling APK to Java with JADX	OK
2025-08-31 02:33:05	Converting DEX to Smali	OK
2025-08-31 02:33:05	Code Analysis Started on - java_source	OK
2025-08-31 02:33:41	Android SBOM Analysis Completed	OK
2025-08-31 02:34:04	Android SAST Completed	OK

2025-08-31 02:34:04	Android API Analysis Started	OK
2025-08-31 02:34:26	Android API Analysis Completed	OK
2025-08-31 02:34:27	Android Permission Mapping Started	OK
2025-08-31 02:34:53	Android Permission Mapping Completed	OK
2025-08-31 02:34:57	Android Behaviour Analysis Started	OK
2025-08-31 02:35:13	Android Behaviour Analysis Completed	OK
2025-08-31 02:35:13	Extracting Emails and URLs from Source Code	OK
2025-08-31 02:35:19	Email and URL Extraction Completed	OK
2025-08-31 02:35:19	Extracting String data from APK	OK
2025-08-31 02:35:19	Extracting String data from Code	OK
2025-08-31 02:35:19	Extracting String values and entropies from Code	OK

2025-08-31 02:35:24	Performing Malware check on extracted domains	OK
2025-08-31 02:35:28	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.

© 2025 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.