MOBSF

ANDROID STATIC ANALYSIS REPORT

Ingenovis (2.14.0)

File Name:	com.ingenovishealth.CandidatePortal_1732148229.apk
Package Name:	com.ingenovishealth.CandidatePortal
Scan Date:	Aug. 30, 2025, 10:11 p.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	8/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
3	13	2	2	1

FILE INFORMATION

File Name: com.ingenovishealth.CandidatePortal_1732148229.apk
Size: 30.01MB
MD5: f8cb1e105b59f133da039749c9ddcc38
SHA1: 6fb2c75a72d338d0f612ac8acca6489bd736fe58
SHA256: 2e8ad7cecf6209f8e87b250aedc772fddd7a41f706f70029a4d8de2e63d96cde

APP INFORMATION

App Name: Ingenovis
Package Name: com.ingenovishealth.CandidatePortal
Main Activity: com.ingenovishealth.CandidatePortal.MainActivity
Target SDK: 34
Min SDK: 22
Max SDK:
Android Version Name: 2.14.0

Android Version Code: 1732148229

APP COMPONENTS

Activities: 8
Services: 9
Receivers: 6
Providers: 7
Exported Activities: 2
Exported Services: 0
Exported Receivers: 2
Exported Providers: 1

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: 2023-03-17 17:33:57+00:00
Valid To: 2053-03-17 17:33:57+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xda6c65d5e0cfc57fb31e3193b93a95976705d5b4
Hash Algorithm: sha256
md5: c479f2733d2990f3e7ff1795421425dc
sha1: e34f2975f2d5f44723f948ad16cddc7696f7e63a
sha256: 996003372af05b301aeb4259f32b1e0655b6e391a06f626b2c1d642e91e591bd
sha512: 839ace98a3e9835c0a50679baa7eb11bb0f82a3fc203eef9c5c79413689407707abc1c4087423c9cbefe5864b79afe0396d632b5eaa8e5e25e6deca0d003420f
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: ef46b8ebeea02d9fc27fe9a49c26916187f4b3fa1f8ed3c60af0a25963ce1878
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
com.ingenovishealth.CandidatePortal.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
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.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>f8cb1e105b59f133da039749c9ddcc38.apk</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table></td></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.BRAND check
Build.DEVICE check
Build.PRODUCT check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
<tr><td>classes2.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></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></td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.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
SIM operator check
network operator name 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>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.ingenovishealth.CandidatePortal.MainActivity	Schemes: @string/deeplink_scheme://, https://, http://, Hosts: auth.dev-ingenovis.com, auth.stage-ingenovis.com, auth.ingenovishealth.com, nurse-portal-ingenovis.dev-ingenovis.com, nurse-portal-ingenovis.stage-ingenovis.com, candidate-portal-ingenovis-future.dev-ingenovis.com, candidate-portal-ingenovis-future.stage-ingenovis.com, www.ingenovishealth.com, @string/applink_host, @string/applink_host_alternate, Paths: /api/auth/login, /jobs, /account/benefits, /account/profile, /account/my-jobs, /account/my-team, /account/requirements-credentials, /account/requirements-credentials/emergency-contact, /account/dashboard, /account/payroll-timesheets, /account/profile/education, /account/profile/license-certificate, /account/profile/work-preferences, /account/profile/agreements, /account/profile/work-history, /account/profile/contact-info, /flow/force-reset, Path Prefixes: /jobs, /account/assignment, Path Patterns: /.*,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.ingenovishealth.CandidatePortal,
com.google.android.gms.tagmanager.TagManagerPreviewActivity	Schemes: tagmanager.c.com.ingenovishealth.CandidatePortal://,

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: **2** | WARNING: **6** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.1-5.1.1, [minSdk=22]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	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
4	Content Provider (com.facebook.FacebookContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity (com.google.android.gms.tagmanager.TagManagerPreviewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	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.
8	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: **0** | WARNING: **5** | INFO: **2** | 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	com/getcapacitor/Logger.java com/getcapacitor/community/inappreview/InAppReview.java io/branch/referral/BranchJsonConfig.java io/branch/referral/BranchLogger.java io/branch/referral/validators/IntegrationValidator.java io/capawesome/capacitorjs/plugins/filepicker/FilePickerPlugin.java io/capawesome/capacitorjs/plugins/firebase/analytics/FirebaseAnalytics.java io/capawesome/capacitorjs/plugins/firebase/messaging/FirebaseMessaging.java io/sentry/SystemOutLogger.java io/sentry/android/core/AndroidLogger.java io/sentry/android/core/SentryLogcatAdapter.java io/sentry/transport/StdoutTransport.java
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/getcapacitor/AppUUID.java com/getcapacitor/Bridge.java com/getcapacitor/Plugin.java io/branch/referral/Branch.java io/branch/referral/BranchPreinstall.java io/branch/referral/PrefHelper.java io/branch/referral/ServerRequest.java io/branch/referral/ServerRequestQueue.java io/branch/referral/UniversalResourceAnalyser.java io/branch/referral/validators/DeepLinkRoutingValidator.java io/sentry/Baggage.java io/sentry/TraceContext.java io/sentry/protocol/User.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/RootChecker.java
4	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/DefaultAndroidEventProcessor.java io/sentry/android/core/internal/util/RootChecker.java
5	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/capacitorjs/plugins/camera/CameraUtils.java com/capacitorjs/plugins/filesystem/Filesystem.java com/getcapacitor/BridgeWebChromeClient.java com/getcapacitor/FileUtils.java io/sentry/android/core/DefaultAndroidEventProcessor.java
6	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/capacitorjs/plugins/camera/CameraUtils.java com/getcapacitor/BridgeWebChromeClient.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	io/sentry/util/StringUtils.java
8	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	io/branch/referral/ShareLinkManager.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/capacitorjs/plugins/browser/Browser.java com/capacitorjs/plugins/pushnotifications/NotificationChannelManager.java com/getcapacitor/AndroidProtocolHandler.java com/getcapacitor/Bridge.java com/getcapacitor/plugin/util/AssetUtil.java io/branch/referral/Branch.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/capacitorjs/plugins/camera/CameraPlugin.java com/capacitorjs/plugins/filesystem/Filesystem.java com/capacitorjs/plugins/filesystem/FilesystemPlugin.java com/getcapacitor/FileUtils.java com/getcapacitor/plugin/util/AssetUtil.java io/sentry/DirectoryProcessor.java io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/PreviousSessionFinalizer.java io/sentry/SentryOptions.java io/sentry/android/core/AndroidOptionsInitializer.java io/sentry/android/core/DefaultAndroidEventProcessor.java io/sentry/android/core/cache/AndroidEnvelopeCache.java io/sentry/cache/CacheStrategy.java io/sentry/cache/CacheUtils.java io/sentry/cache/EnvelopeCache.java io/sentry/instrumentation/file/FileIOSpanManager.java
00013	Read file and put it into a stream	file	com/capacitorjs/plugins/filesystem/Filesystem.java com/getcapacitor/AndroidProtocolHandler.java io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/PreviousSessionFinalizer.java io/sentry/SentryEnvelopeItem.java io/sentry/cache/CacheStrategy.java io/sentry/cache/CacheUtils.java io/sentry/cache/EnvelopeCache.java io/sentry/config/FilesystemPropertiesLoader.java io/sentry/instrumentation/file/FileInputStreamInitData.java io/sentry/instrumentation/file/SentryFileInputStream.java

RULE ID	BEHAVIOUR	LABEL	FILES
00012	Read data and put it into a buffer stream	file	io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/SentryEnvelopeItem.java io/sentry/cache/CacheStrategy.java io/sentry/cache/EnvelopeCache.java io/sentry/config/FilesystemPropertiesLoader.java
00072	Write HTTP input stream into a file	command network file	com/getcapacitor/plugin/util/AssetUtil.java
00089	Connect to a URL and receive input stream from the server	command network	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java io/sentry/transport/HttpConnection.java
00030	Connect to the remote server through the given URL	network	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java io/sentry/transport/HttpConnection.java
00094	Connect to a URL and read data from it	command network	com/capacitorjs/plugins/filesystem/Filesystem.java com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java
00108	Read the input stream from given URL	network command	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java
00096	Connect to a URL and set request method	command network	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/HttpRequestHandler.java io/sentry/transport/HttpConnection.java

RULE ID	BEHAVIOUR	LABEL	FILES
00123	Save the response to JSON after connecting to the remote server	network command	com/getcapacitor/plugin/util/CapacitorHttpUrlConnection.java com/getcapacitor/plugin/util/HttpRequestHandler.java
00109	Connect to a URL and get the response code	network command	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/HttpRequestHandler.java io/sentry/transport/HttpConnection.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/capacitorjs/plugins/browser/BrowserPlugin.java com/capacitorjs/plugins/camera/CameraPlugin.java com/getcapacitor/Bridge.java io/branch/referral/Branch.java io/branch/referral/validators/DeepLinkRoutingValidator.java io/capawesome/capacitorjs/plugins/appupdate/AppUpdatePlugin.java nl/raphael/settings/NativeSettingsPlugin.java
00091	Retrieve data from broadcast	collection	com/capacitorjs/plugins/pushnotifications/PushNotificationsPlugin.java com/getcapacitor/Bridge.java io/branch/referral/Branch.java io/capawesome/capacitorjs/plugins/firebase/messaging/FirebaseMessagingPlugin.java
00125	Check if the given file path exist	file	com/capacitorjs/plugins/camera/CameraPlugin.java com/getcapacitor/Bridge.java
00078	Get the network operator name	collection telephony	io/branch/referral/SystemObserver.java
00191	Get messages in the SMS inbox	sms	com/getcapacitor/FileUtils.java io/branch/coroutines/InstallReferrersKt.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	io/branch/referral/Branch.java nl/raphael/settings/NativeSettingsPlugin.java

RULE ID	BEHAVIOUR	LABEL	FILES
00003	Put the compressed bitmap data into JSON object	camera	io/branch/referral/network/BranchRemoteInterfaceUrlConnection.java
00054	Install other APKs from file	reflection	com/capacitorjs/plugins/camera/CameraPlugin.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/capacitorjs/plugins/camera/CameraPlugin.java
00024	Write file after Base64 decoding	reflection file	com/capacitorjs/plugins/camera/CameraPlugin.java com/capacitorjs/plugins/filesystem/Filesystem.java
00153	Send binary data over HTTP	http	com/getcapacitor/plugin/util/CapacitorHttpUrlConnection.java
00192	Get messages in the SMS inbox	sms	com/getcapacitor/FileUtils.java
00028	Read file from assets directory	file	com/getcapacitor/FileUtils.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/124684004147/namespaces/firebase:fetch?key=AIzaSyDUQVMryNR55iLf7mlV_qfy5dOvqrTC6ZQ. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.VIBRATE
Other Common Permissions	3/44	com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.c2dm.permission.RECEIVE

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

DOMAIN	STATUS	GEOLOCATION
help.branch.io	ok	**IP:** 104.18.21.218 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api3-eu.branch.io	ok	**IP:** 18.155.173.13 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api.branch.io	ok	**IP:** 18.238.109.24 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
capacitorjs.com	ok	**IP:** 172.67.203.214 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
bnc.lt	ok	**IP:** 18.238.109.120 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api2.branch.io	ok	**IP:** 18.238.109.117 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
cdn.branch.io	ok	**IP:** 18.238.109.80 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
play.google.com	ok	**IP:** 142.250.188.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
branch.app.link	ok	**IP:** 18.238.109.80 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

HARDCODED SECRETS

POSSIBLE SECRETS
"branch_key" : "key_live_juiJpS3uGEAl5npqPpVvnfmfDEdgX2Ca"
"branch_test_key" : "key_test_lFjVjUXBRysc6bkCLoKEClalurog68Br"
"facebook_client_token" : "4ef30f79bf656d6b1b11a318dee0002d"
"google_api_key" : "AIzaSyDUQVMryNR55iLf7mlV_qfy5dOvqrTC6ZQ"
"google_crash_reporting_api_key" : "AIzaSyDUQVMryNR55iLf7mlV_qfy5dOvqrTC6ZQ"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
c56fb7d591ba6704df047fd98f535372fea00211
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
9b8f518b086098de3d77736f9458a3d2f6f95a37
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
cc2751449a350f668590264ed76692694a80308a

PLAYSTORE INFORMATION

Title: Ingenovis Health

Score: 4.61 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.ingenovishealth.CandidatePortal

Developer Details: Ingenovis Health, Ingenovis+Health, None, https://www.ingenovishealth.com/contact-us, nursehelpdesk@fastaff.com,

Release Date: Apr 20, 2023 **Privacy Policy:** Privacy link

Description:

The Ingenovis Health App combines the Trustaff, Fastaff and USN mobile apps so you can access more travel nursing and allied jobs in one place, apply with one click and maintain a single profile. The new home for healthcare talent is here. Experience the Ingenovis Health App difference: • Search real-time healthcare jobs from Trustaff, Fastaff and U.S. Nursing with advanced search filtering • Use One-Click Apply on jobs of interest to connect with a recruiter • Easily update your profile across all three companies with a single login • Complete your professional skills checklists and upload documents in one place • Stay connected with your recruiter and support team during your job search and beyond Download the Ingenovis Health App now to connect to an ecosystem of opportunity tailored to you, and a personal team who will support you through every phase of your career.

SCAN LOGS

Timestamp	Event	Error
2025-08-30 22:11:49	Generating Hashes	OK
2025-08-30 22:11:49	Extracting APK	OK
2025-08-30 22:11:49	Unzipping	OK

2025-08-30 22:11:49	Parsing APK with androguard	OK
2025-08-30 22:11:49	Extracting APK features using aapt/aapt2	OK
2025-08-30 22:11:49	Getting Hardcoded Certificates/Keystores	OK
2025-08-30 22:11:51	Parsing AndroidManifest.xml	OK
2025-08-30 22:11:51	Extracting Manifest Data	OK
2025-08-30 22:11:51	Manifest Analysis Started	OK
2025-08-30 22:11:51	Performing Static Analysis on: Ingenovis (com.ingenovishealth.CandidatePortal)	OK
2025-08-30 22:11:52	Fetching Details from Play Store: com.ingenovishealth.CandidatePortal	OK
2025-08-30 22:11:52	Checking for Malware Permissions	OK
2025-08-30 22:11:52	Fetching icon path	OK
2025-08-30 22:11:52	Library Binary Analysis Started	OK

2025-08-30 22:11:52	Reading Code Signing Certificate	OK
2025-08-30 22:11:53	Running APKiD 2.1.5	OK
2025-08-30 22:11:57	Detecting Trackers	OK
2025-08-30 22:12:00	Decompiling APK to Java with JADX	OK
2025-08-30 22:12:18	Converting DEX to Smali	OK
2025-08-30 22:12:18	Code Analysis Started on - java_source	OK
2025-08-30 22:12:20	Android SBOM Analysis Completed	OK
2025-08-30 22:12:28	Android SAST Completed	OK
2025-08-30 22:12:28	Android API Analysis Started	OK
2025-08-30 22:12:33	Android API Analysis Completed	OK
2025-08-30 22:12:33	Android Permission Mapping Started	OK

2025-08-30 22:12:38	Android Permission Mapping Completed	OK
2025-08-30 22:12:38	Android Behaviour Analysis Started	OK
2025-08-30 22:12:44	Android Behaviour Analysis Completed	OK
2025-08-30 22:12:44	Extracting Emails and URLs from Source Code	OK
2025-08-30 22:12:45	Email and URL Extraction Completed	OK
2025-08-30 22:12:45	Extracting String data from APK	OK
2025-08-30 22:12:45	Extracting String data from Code	OK
2025-08-30 22:12:45	Extracting String values and entropies from Code	OK
2025-08-30 22:12:48	Performing Malware check on extracted domains	OK
2025-08-30 22:12:49	Saving to Database	OK

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.