ANDROID STATIC ANALYSIS REPORT

CG ePass (1.0.6)

File Name:	CG ePass 1.0.6.apk
Package Name:	com.allsoft.corona
Average CVSS Score:	6.3
App Security Score:	10/100 (CRITICAL RISK)
Trackers Detection:	2/285

FILE INFORMATION

File Name: CG ePass 1.0.6.apk
Size: 8.86MB
MD5: 4db2d29699ce53d5a3e980ee098064a7
SHA1: 6ae554aabdb0ed72ca27314d30357241f26923e7
SHA256: dc2dad997b46de3266b3021f760ff54ae98795e2b2dda20ba47a510ee45c30bc

APP INFORMATION

App Name: CG ePass
Package Name: com.allsoft.corona
Main Activity: com.allsoft.corona.views.SplashScreenActivity
Target SDK: 28
Min SDK: 19
Max SDK:
Android Version Name: 1.0.6
Android Version Code: 19

APP COMPONENTS

Activities: 28
Services: 8
Receivers: 5
Providers: 7
Exported Activities: 2
Exported Services: 2
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-03-28 08:14:03+00:00
Valid To: 2050-03-28 08:14:03+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xe8d4529bb26059f84597779e543d5b9d9b422903
Hash Algorithm: sha256
md5: 997eae18d607d4999ae4a406a8134ac4
sha1: ef96dab3886adcbc9f81cfd52b635a8ab51bdbf5
sha256: 07b7248010d542271d7cad7d6cc6c95b03737e3bdce839e8fda62730be270b3a
sha512:
```

460f6fa433b0451f1a4ddde12286bff7fe58775882e8014d6f19aeed5e9858ef62f9b7ac45db3131c0c05faca8189e85f3b20f8c970221ef95f881538ddd2d1a

PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 57ee2689f2beaf0d97553857a7241979e5669704877aafb4ba4e1b41224ffb94

Certificate Status: Good
Description: Certificate looks good.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
android.permission.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	dangerous	Unknown permission from android reference	Unknown permission from android reference

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.MANUFACTURER check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>classes2.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.BOARD 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>dx</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.allsoft.corona.views.SplashScreenActivity	Schemes: http://, Hosts: jewelfactory.in, Path Patterns: /android,
com.facebook.CustomTabActivity	Schemes: @string/facebook_login_protocol_scheme://,

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
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.
Application Data can be Backed up [android:allowBackup=true]	medium	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.
Service (com.allsoft.corona.services.MyFirebaseMessagingService) is not Protected. An intent-filter exists.	high	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.
Broadcast Receiver (com.allsoft.corona.receivers.ConnectivityReceiver) is not Protected. An intent-filter exists.	high	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.
Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
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]	high	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.

ISSUE	SEVERITY	DESCRIPTION
Launch Mode of Activity (com.google.firebase.auth.internal.FederatedSignInActivity) is not standard.	high	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.
Activity (com.google.firebase.auth.internal.FederatedSignInActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.firebase.auth.api.gms.permission.LAUNCH_FEDERATED_SIGN_IN [android:exported=true]	high	An Activity 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.
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]	high	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.
Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	high	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

ISSUE	SEVERITY	STANDARDS	FILES
			io/opencensus/metrics/AutoValue_MetricOptions.java io/opencensus/metrics/AutoValue_LabelKey.java io/opencensus/metrics/AutoValue_LabelValue.java io/opencensus/metrics/export/AutoValue_Value_ValueSummary.java io/opencensus/metrics/export/AutoValue_Distribution.java io/opencensus/metrics/export/AutoValue_Summary_Snapshot.java io/opencensus/metrics/export/AutoValue_TimeSeries.java io/opencensus/metrics/export/AutoValue_Summary.java io/opencensus/metrics/export/AutoValue_Point.java io/opencensus/metrics/export/AutoValue_Distribution_BucketOptions_ExplicitOptions.java io/opencensus/metrics/export/AutoValue_Value_ValueDistribution.java io/opencensus/metrics/export/AutoValue_Metric.java io/opencensus/metrics/export/AutoValue_MetricDescriptor.java io/opencensus/metrics/export/AutoValue_Distribution_Bucket.java io/opencensus/metrics/data/AutoValue_AttachmentValue_AttachmentValueString.java io/opencensus/metrics/data/AutoValue_Exemplar.java io/opencensus/trace/AutoValue_Link.java io/opencensus/trace/AutoValue_Annotation.java io/opencensus/trace/AutoValue_AttributeValue_AttributeValueBoolean.java io/opencensus/trace/AutoValue_AttributeValue_AttributeValueDouble.java io/opencensus/trace/AutoValue_NetworkEvent.java io/opencensus/trace/AutoValue_AttributeValue_AttributeValueString.java io/opencensus/trace/AutoValue_Tracestate_Entry.java io/opencensus/trace/AutoValue_EndSpanOptions.java io/opencensus/trace/AutoValue_AttributeValue_AttributeValueLong.java io/opencensus/trace/AutoValue_MessageEvent.java io/opencensus/trace/AutoValue_Tracestate.java io/opencensus/trace/config/AutoValue_T

ISSUE	SEVERITY	STANDARDS	FILES
This App uses Java Hash Code. It's a weak hash function and should never be used in Secure Crypto Implementation.	warning	**CVSS V2:** 2.3 (low) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP MASVS:** MSTG-CRYPTO-4	io/opencensus/trace/config/AutoValue_TraceParams.java io/opencensus/trace/export/AutoValue_SampledSpanStore_Summary.java io/opencensus/trace/export/AutoValue_RunningSpanStore_Filter.java io/opencensus/trace/export/AutoValue_SpanData_TimedEvent.java io/opencensus/trace/export/AutoValue_SpanData_Attributes.java io/opencensus/trace/export/AutoValue_SampledSpanStore_LatencyFilter.java io/opencensus/trace/export/AutoValue_SpanData.java io/opencensus/trace/export/AutoValue_SpanData_TimedEvents.java io/opencensus/trace/export/AutoValue_SpanData_Links.java io/opencensus/trace/export/AutoValue_SampledSpanStore_ErrorFilter.java io/opencensus/trace/export/AutoValue_RunningSpanStore_Summary.java io/opencensus/trace/export/AutoValue_SampledSpanStore_PerSpanNameSummary.java io/opencensus/tags/AutoValue_TagKey.java io/opencensus/tags/AutoValue_TagMetadata.java io/opencensus/tags/TagContext.java io/opencensus/tags/AutoValue_TagValue.java io/opencensus/tags/AutoValue_Tag.java io/opencensus/resource/AutoValue_Resource.java io/opencensus/stats/AutoValue_ViewData_AggregationWindowData_CumulativeData.java io/opencensus/stats/AutoValue_Measure_MeasureDouble.java io/opencensus/stats/AutoValue_ViewData.java io/opencensus/stats/AutoValue_Measurement_MeasurementLong.java io/opencensus/stats/AutoValue_View_AggregationWindow_Interval.java io/opencensus/stats/AutoValue_ViewData_AggregationWindowData_IntervalData.java io/opencensus/stats/AutoValue_AggregationData_DistributionData.java io/opencensus/stats/AutoValue_View.java io/opencensus/stats/AutoValue_Measure_MeasureLong.java io/opencensus/stats/AutoValue_Aggregation_Distribution.java io/opencensus/stats/AutoValue_Measurement_MeasurementDouble.java io/opencensus/stats/AutoValue_BucketBoundaries.java io/opencensus/stats/AutoValue_View_Name.java io/grpc/Status.java

ISSUE	SEVERITY	STANDARDS	FILES
			io/grpc/LoadBalancerProvider.java io/grpc/EquivalentAddressGroup.java io/grpc/PersistentHashArrayMappedTrie.java io/grpc/Metadata.java io/grpc/ConnectivityStateInfo.java io/grpc/inprocess/InProcessSocketAddress.java io/grpc/perfmark/PerfTag.java io/grpc/okhttp/internal/framed/Header.java com/squareup/picasso/RemoteViewsAction.java com/otaliastudios/cameraview/video/encoding/TextureMediaEncoder.java com/allsoft/corona/utils/FileCache.java com/firebase/ui/auth/IdpResponse.java com/firebase/ui/auth/AuthUI.java com/firebase/ui/auth/ui/idp/WelcomeBackIdpPrompt.java com/firebase/ui/auth/ui/idp/AuthMethodPickerActivity.java com/firebase/ui/auth/ui/idp/SingleSignInActivity.java com/firebase/ui/auth/ui/phone/PhoneVerification.java com/firebase/ui/auth/util/data/ProviderUtils.java com/firebase/ui/auth/data/model/CountryInfo.java com/firebase/ui/auth/data/model/Resource.java com/firebase/ui/auth/data/model/User.java com/firebase/ui/auth/data/remote/SignInKickstarter.java
Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-312 - Cleartext Storage of Sensitive Information **OWASP Top 10:** M9: Reverse Engineering **OWASP MASVS:** MSTG-STORAGE-14	io/opencensus/metrics/AutoValue_LabelKey.java io/opencensus/trace/AutoValue_Tracestate_Entry.java io/opencensus/tags/AutoValue_Tag.java io/grpc/internal/TransportFrameUtil.java io/grpc/internal/ServiceConfigUtil.java io/grpc/internal/DnsNameResolver.java com/allsoft/corona/security/Security.java com/allsoft/corona/utils/AppConstants.java com/allsoft/corona/utils/Constants.java com/firebase/ui/auth/IdpResponse.java com/firebase/ui/auth/ui/phone/PhoneNumberVerificationHandler.java com/firebase/ui/auth/ui/email/EmailLinkErrorRecoveryActivity.java com/firebase/ui/auth/util/data/EmailLinkPersistenceManager.java

ISSUE	SEVERITY	STANDARDS	FILES
The App uses an insecure Random Number Generator.	high	**CVSS V2:** 7.5 (high) **CWE:** CWE-330 - Use of Insufficiently Random Values **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-6	io/opencensus/trace/SpanId.java io/opencensus/trace/TraceId.java io/grpc/util/RoundRobinLoadBalancer.java io/grpc/internal/RetriableStream.java io/grpc/internal/ExponentialBackoffPolicy.java io/grpc/internal/DnsNameResolver.java io/grpc/okhttp/OkHttpClientTransport.java com/otaliastudios/cameraview/filters/GrainFilter.java com/otaliastudios/cameraview/filters/DocumentaryFilter.java com/otaliastudios/cameraview/filters/LomoishFilter.java com/otaliastudios/cameraview/video/encoding/AudioNoise.java com/allsoft/corona/fragments/corona/DBEPassV2Fragment.java com/allsoft/corona/fragments/corona/DBEPassFragment.java com/allsoft/corona/services/MyFirebaseMessagingService.java com/firebase/ui/auth/util/data/SessionUtils.java
			io/grpc/android/AndroidChannelBuilder.java io/grpc/okhttp/internal/Platform.java me/zhanghai/android/materialprogressbar/BaseProgressLayerDrawable.java me/zhanghai/android/materialprogressbar/MaterialProgressBar.java com/squareup/picasso/StatsSnapshot.java com/squareup/picasso/Utils.java com/otaliastudios/cameraview/CameraLogger.java com/otaliastudios/opengl/core/EglConfigChooser.java com/otaliastudios/opengl/core/Egloo.java com/otaliastudios/opengl/core/EglCore.java com/otaliastudios/opengl/core/EglContextFactory.java com/allsoft/corona/App.java com/allsoft/corona/fragments/corona/DBEPassV2Fragment.java com/allsoft/corona/fragments/corona/DBCFeedsFragment.java com/allsoft/corona/fragments/corona/DBVerifyEPassFragment.java com/allsoft/corona/fragments/corona/DBEPassFragment.java com/allsoft/corona/network/HTTPRequestHelper.java com/allsoft/corona/network/APIProcessor.java

ISSUE	SEVERITY	STANDARDS	FILES
The App logs information. Sensitive information should never be logged.	info	**CVSS V2:** 7.5 (high) **CWE:** CWE-532 - Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3	com/allsoft/corona/utils/SharedPreferenceManager.java com/allsoft/corona/utils/FileUtils.java com/allsoft/corona/utils/Logger.java com/allsoft/corona/utils/TypefaceUtil.java com/allsoft/corona/utils/AppHelper.java com/allsoft/corona/utils/CryptLib.java com/allsoft/corona/utils/Log.java com/allsoft/corona/utils/FileManager.java com/allsoft/corona/utils/ForceUpdateChecker.java com/allsoft/corona/utils/BottomNavigationViewHelper.java com/allsoft/corona/views/PhoneNumberAuthentication.java com/allsoft/corona/views/FeedsActivity.java com/allsoft/corona/views/PoliceVerificationActivity.java com/allsoft/corona/handlers/AlertDialogHandler.java com/allsoft/corona/services/MyFirebaseMessagingService.java com/firebase/ui/auth/AuthUI.java com/firebase/ui/auth/viewmodel/ResourceObserver.java com/firebase/ui/auth/viewmodel/smartlock/SmartLockHandler.java com/firebase/ui/auth/ui/email/EmailLinkFragment.java com/firebase/ui/auth/ui/credentials/CredentialSaveActivity.java com/firebase/ui/auth/util/data/TaskFailureLogger.java com/firebase/ui/auth/data/remote/GoogleSignInHandler.java com/github/barteksc/pdfviewer/PDFView.java com/shockwave/pdfium/PdfiumCore.java com/journeyapps/barcodescanner/DecoderThread.java com/journeyapps/barcodescanner/CameraPreview.java com/journeyapps/barcodescanner/CaptureManager.java com/journeyapps/barcodescanner/camera/CenterCropStrategy.java com/journeyapps/barcodescanner/camera/CameraInstance.java com/journeyapps/barcodescanner/camera/PreviewScalingStrategy.java com/journeyapps/barcodescanner/camera/AutoFocusManager.java com/journeyapps/barcodescanner/camera/CameraManager.java com/journeyapps/barcodescanner/camera/FitCenterStrategy.java com/journeyapps/barcodescanner/camera/LegacyPreviewScalingStrategy.java

ISSUE	SEVERITY	STANDARDS	FILES
MD5 is a weak hash known to have hash collisions.	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-4	io/grpc/okhttp/internal/Util.java com/allsoft/corona/security/Security.java com/allsoft/corona/utils/SecurityUtil.java com/allsoft/corona/utils/CryptLib.java
App can read/write to External Storage. Any App can read data written to External Storage.	high	**CVSS V2:** 5.5 (medium) **CWE:** CWE-276 - Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2	com/allsoft/corona/fragments/corona/DBEPassV2Fragment.java com/allsoft/corona/fragments/corona/DBEPassFragment.java com/allsoft/corona/constants/AppConstants.java com/allsoft/corona/utils/FileUtils.java com/allsoft/corona/utils/Logger.java com/allsoft/corona/utils/FileCache.java com/allsoft/corona/utils/Utils.java com/allsoft/corona/utils/FileManager.java
Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-295 - Improper Certificate Validation **OWASP Top 10:** M3: Insecure Communication **OWASP MASVS:** MSTG-NETWORK-3	com/allsoft/corona/network/HTTPRequestHelper.java
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.	high	**CVSS V2:** 5.9 (medium) **CWE:** CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') **OWASP Top 10:** M7: Client Code Quality	com/allsoft/corona/utils/DbMigrationHelper.java
App creates temp file. Sensitive information should never be written into a temp file.	high	**CVSS V2:** 5.5 (medium) **CWE:** CWE-276 - Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2	com/journeyapps/barcodescanner/CaptureManager.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
covid.apollo247.com	good	**IP:** 13.71.124.125 **Country:** India **Region:** Tamil Nadu **City:** Chennai **Latitude:** 13.08784 **Longitude:** 80.278473 **View:** Google Map
phone.firebase	good	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
cgcovid19.in	good	**IP:** 13.126.44.28 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.01441 **Longitude:** 72.847939 **View:** Google Map
github.com	good	**IP:** 13.236.229.21 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map
www.covid19india.org	good	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Indiana **City:** Francisco **Latitude:** 38.333332 **Longitude:** -87.44722 **View:** Google Map
play.google.com	good	**IP:** 216.58.196.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
raipur-police.firebaseio.com	good	**IP:** 35.201.97.85 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

URLS

URL	FILE
https://github.com/grpc/grpc-java/issues/5015	io/grpc/internal/ManagedChannelImpl.java
https://play.google.com/store/apps/details?id=com.allsoft.corona	com/allsoft/corona/App.java
http://cgcovid19.in/sendsms.php?otp=	com/allsoft/corona/fragments/corona/DBEPassV2Fragment.java

URL	FILE
http://cgcovid19.in/sendsms.php?otp=	com/allsoft/corona/fragments/corona/DBEPassFragment.java
https://covid.apollo247.com	com/allsoft/corona/fragments/corona/DBSelfDiagnosticFragment.java
https://www.covid19india.org/	com/allsoft/corona/fragments/corona/DBCHomeFragment.java
https://covid.apollo247.com	com/allsoft/corona/views/SelfDiagnosisActivity.java
https://github.com/firebase/FirebaseUI-Android/releases/tag/6.2.0 https://github.com/firebase/FirebaseUI-Android/blob/master/auth/README.md#facebook	com/firebase/ui/auth/AuthUI.java
https://github.com https://phone.firebase	com/firebase/ui/auth/util/data/ProviderUtils.java
https://raipur-police.firebaseio.com	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://raipur-police.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
nk@cgepass.in	com/allsoft/corona/App.java
info@domain.com priya@photogurus.com	com/allsoft/corona/utils/FileUtils.java

TRACKERS

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

PLAYSTORE INFORMATION

Title: CG Covid-19 ePass

Score: 3.4827585 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** 4.4 and up **Category:** Productivity **Play Store URL:** com.allsoft.corona

Developer Details: AllSoft Consulting, AllSoft+Consulting, ASC AllSoft IT Consulting Pvt. Ltd. #26, Third Floor, Magneto Offizo, G E Road Raipur, Chhattisgarh, INDIA, https://raipur.gov.in/, helpdesk.rscl@gmail.com,

Release Date: Mar 28, 2020 **Privacy Policy:** Privacy link

Description:

This is an official app of Government of Chhattisgarh. The World is fighting with the “COVID-19” Pandemic and to take on this battle in State of Chhattisgarh, the State Government has imposed a complete lock-down in the entire State. This lockdown has directed people of Chhattisgarh to stay put in their homes as a preventive measure to stop the spread of COVID-19. Government of Chhattisgarh has launched this app to issue State-wide and Intra-district e-Pass for vehicular movement during the lock-down period to enable the seamless transportation of essential commodities like Food grains, Vegetables, Fruits, Milk, Fuel etc. within the State of Chhattisgarh. The applicant can obtain an e-Pass by submitting Photograph, Id Proof (Aadhaar Card) and Business proof. The Applicant will be able to select the travel date, time and destination. Health officials and Government employees/ staff need not to apply for e-Pass from this mobile app. They will follow the prevalent protocol given by Chhattisgarh Government. This mobile app will help the State Administration to serve people residing in the State of Chhattisgarh and keep them safe in their homes during these times of hardship.

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

Report Generated by - MobSF v3.0.8 Beta

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.