MobSF

ANDROID STATIC ANALYSIS REPORT

Coronavirus (1.0.2)

File Name:	Coronavirus 1.0.2.apk
Package Name:	au.gov.health.covid19
Average CVSS Score:	6.0
App Security Score:	30/100 (HIGH RISK)
Trackers Detection:	1/285

FILE INFORMATION

File Name: Coronavirus 1.0.2.apk
Size: 7.11MB
MD5: 1c26a4bb5b5cfc7b2967eedf9173d719
SHA1: 0415bda245d0f56059538bfab27a53e6dcb135af
SHA256: 413fe27e19e200da743ddb9d22e99e2fbc5f5b5a03537e2f9a9cb6c7ad1337ab

APP INFORMATION

App Name: Coronavirus
Package Name: au.gov.health.covid19
Main Activity: au.gov.health.covid19.loading.LoadingActivity
Target SDK: 29
Min SDK: 23
Max SDK:
Android Version Name: 1.0.2
Android Version Code: 10

APP COMPONENTS

Activities: 4
Services: 7
Receivers: 4
Providers: 2
Exported Activities: 1
Exported Services: 0
Exported Receivers: 2
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: 2020-03-21 01:32:11+00:00
Valid To: 2050-03-21 01:32:11+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x4b9ec9ea0f9979a95b4d52c4fef8086e4b094716
Hash Algorithm: sha256
md5: 1ce99155d92f1e8086cc4b722e73e605
sha1: 670058ac3e2a3197c1b7f3f26181c0139233f864
sha256: 52acc3e336d69749863b917aabc5ad4150ea704172f907893aea0d8ae67f4afa
sha512:
8389c31b04cc997b2ba85a292cf184274c7931fa7a481a57691ee8487d76e05810d89fe6a204b581752845705fa82e056cf994110d545d1706bf6b8816bb3643

PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: c26b8cdf65f54c0a28e06b0c17bc6314ad6d552b663b5241ad479ccff226b6af

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.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_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.

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</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 Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
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.
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.

ISSUE	SEVERITY	DESCRIPTION
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.
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.

CODE ANALYSIS

ISSUE	SEVERITY	STANDARDS	FILES
			kotlinx/coroutines/JobCancellationException.java kotlinx/coroutines/CoroutineContextKt.java kotlinx/coroutines/CoroutineName.java kotlinx/coroutines/DebugKt.java kotlinx/coroutines/internal/ThreadLocalKey.java kotlinx/coroutines/channels/ValueOrClosed.java 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.j

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	ava 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_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/Status.java 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 io/noties/markwon/Prop.java io/noties/markwon/image/AsyncDrawableScheduler.java au/gov/health/covid19/config/Preamble.java au/gov/health/covid19/config/Banners.java au/gov/health/covid19/config/CovidLink.java au/gov/health/covid19/config/Contact.java au/gov/health/covid19/config/AdviceCategory.java au/gov/health/covid19/config/ConfigSections.java au/gov/health/covid19/config/Advice.java au/gov/health/covid19/config/Resource.java au/gov/health/covid19/config/CovidFirebaseMessagingService.java au/gov/health/covid19/config/ContactDetail.java au/gov/health/covid19/config/FormFlow.java au/gov/health/covid19/config/WebLinkContent.java au/gov/health/covid19/config/EssentialInformation.java au/gov/health/covid19/config/Banner.java au/gov/health/covid19/config/AlertStatus.java au/gov/health/covid19/config/Config.java au/gov/health/covid19/config/Setting.java au/gov/health/covid19/config/ResourceCollection.java au/gov/health/covid19/status/StatusItem.java au/gov/health/covid19/status/CoronavirusStatus.java au/gov/health/covid19/news/NewsItem.java au/gov/health/covid19/isolation/landing/IsolationLandingDetail.java au/gov/health/covid19/isolation/landing/IsolationLandingDetailState.java au/gov/health/covid19/isolation/result/IsolationResultText.java au/gov/health/covid19/isolation/flow/IsolationFlowRegisterFragment$onCreateView$$inlined$apply$lambda$1.java au/gov/health/covid19/isolation/flow/IsolationFlowTestFragment$onCreateView$$inlined$let$lambda$1.java au/gov/health/covid19/isolation/flow/IsolationRegistration.java au/gov/health/covid19/privacypolicy/PrivacyPolicyDetails.java com/bumptech/glide/util/Util.java com/bumptech/glide/util/MultiClassKey.java com/bumptech/glide/util/CachedHashCodeArrayMap.java com/bumptech/glide/signature/MediaStoreSignature.java com/bumptech/glide/signature/ObjectKey.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/Options.java com/bumptech/glide/load/MultiTransformation.java com/bumptech/glide/load/model/GlideUrl.java com/bumptech/glide/load/model/ModelCache.java com/bumptech/glide/load/model/LazyHeaders.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/DrawableTransformation.java com/bumptech/glide/load/resource/bitmap/BitmapDrawableTransformation.java com/bumptech/glide/load/resource/gif/GifDrawableTransformation.java com/bumptech/glide/load/engine/EngineKey.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineJob.java

ISSUE	SEVERITY	STANDARDS	FILES
			com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/load/engine/prefill/PreFillType.java com/bumptech/glide/load/engine/bitmap_recycle/AttributeStrategy.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/SizeConfigStrategy.java com/bumptech/glide/request/SingleRequest.java
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	kotlinx/coroutines/scheduling/CoroutineScheduler.java 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
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 au/gov/health/covid19/loading/LoadingActivity.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/load/engine/EngineResource.java
			io/grpc/android/AndroidChannelBuilder.java io/grpc/okhttp/internal/Platform.java io/noties/markwon/PrecomputedTextSetterCompat.java io/noties/markwon/LinkResolverDef.java au/gov/health/covid19/MainActivity.java au/gov/health/covid19/loading/LoadingViewModel$start$4.java au/gov/health/covid19/loading/LoadingViewModel.java au/gov/health/covid19/loading/LoadingActivity$onCreate$4.java au/gov/health/covid19/status/StatusViewModel.java au/gov/health/covid19/essential/EssentialInformationViewModel.java au/gov/health/covid19/news/NewsViewModel.java au/gov/health/covid19/isolation/landing/IsolationLandingViewModel$$special$$inlined$let$lambda$1.java au/gov/health/covid19/isolation/flow/IsolationViewModel$updateIsolationRegistration$locationObserver$1$onChanged$$inlined$let$lambda$1.java au/gov/health/covid19/isolation/flow/IsolationViewModel$updateIsolationRegistration$locationObserver$1.java au/gov/health/covid19/isolation/flow/IsolationViewModel$updateIsolationRegistration$locationObserver$1$onChanged$$inlined$let$lambda$2.java au/gov/health/covid19/isolation/flow/IsolationViewModel$lAuthenticatedObserver$1.java au/gov/health/covid19/isolation/flow/IsolationViewModel.java com/bumptech/glide/Glide.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/bumptech/glide/signature/ApplicationVersionSignature.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/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/resource/ImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.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
SHA-1 is a weak hash known to have hash collisions.	high	**CVSS V2:** 5.9 (medium) **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
App can write to App Directory. Sensitive Information should be encrypted.	info	**CVSS V2:** 3.9 (low) **CWE:** CWE-276 - Incorrect Default Permissions **OWASP MASVS:** MSTG-STORAGE-14	au/gov/health/covid19/CoronavirusApplication.java
This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	**CVSS V2:** 0 (info) **OWASP MASVS:** MSTG-STORAGE-10	au/gov/health/covid19/settings/SettingsFragment$onCreateView$gestureDetector$1.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
health.gov.au	good	**IP:** 103.29.195.64 **Country:** Australia **Region:** Australian Capital Territory **City:** Waramanga **Latitude:** -35.35297 **Longitude:** 149.062134 **View:** Google Map
health-covid-19.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

DOMAIN	STATUS	GEOLOCATION
www.health.gov.au	good	**IP:** 23.213.128.54 **Country:** Australia **Region:** Victoria **City:** Melbourne **Latitude:** -37.813999 **Longitude:** 144.963318 **View:** Google Map
github.com	good	**IP:** 52.64.108.95 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map
android.asset	good	No Geolocation information available.

URLS

URL	FILE
https://github.com/grpc/grpc-java/issues/5015	io/grpc/internal/ManagedChannelImpl.java
file:///android_asset/ https://android.asset/	io/noties/markwon/urlprocessor/UrlProcessorAndroidAssets.java
https://www.health.gov.au/news/health-alerts/novel-coronavirus-2019-ncov-health-alert/government-response-to-the-covid-19-outbreak	au/gov/health/covid19/response/GovernmentResponseViewModel.java
https://health.gov.au	au/gov/health/covid19/config/AdviceCategory.java
https://www.health.gov.au/resources/publications/coronavirus-covid-19-isolation-guidance)'	au/gov/health/covid19/isolation/landing/IsolationLandingDetail.java
https://www.health.gov.au/resources/publications/coronavirus-covid-19-isolation-guidance)'	au/gov/health/covid19/isolation/result/IsolationResultFragment.java
https://www.health.gov.au/using-our-websites/privacy#covid-location)	au/gov/health/covid19/isolation/location/LocationPermissionFragment.java
file:///android_asset/	com/bumptech/glide/load/model/AssetUriLoader.java
data:image	com/bumptech/glide/load/model/DataUrlLoader.java
https://health-covid-19.firebaseio.com https://www.health.gov.au/using-our-websites/privacy https://www.health.gov.au/using-our-websites/privacy)	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://health-covid-19.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

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

PLAYSTORE INFORMATION

Title: Coronavirus Australia

Score: 3.775 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** 6.0 and up **Category:** Health & Fitness **Play Store URL:** au.gov.health.covid19

Developer Details: DTA App Developer, DTA+App+Developer, None, http://health.gov.au, info@health.gov.au,

Release Date: None **Privacy Policy:** Privacy link

Description:

You can use the Australian Government Coronavirus app to: - stay up to date with the official information and advice - important health advice to help stop the spread and stay healthy - get a quick snapshot of the current official status within Australia - check your symptoms if you are concerned about yourself or someone else - find relevant contact information - access updated information from the Australian Government - receive push notifications of urgent information and updates Trusted, Australian information All information in the Australian Government Coronavirus app is sourced from Australia's leading health organisations and has undergone a quality assurance process so people can know it is safe, appropriate and relevant for Australians. Disclaimer Whilst this app has been reviewed for clinical accuracy, the content is not a substitute for professional advice and should not be used as an alternative to professional healthcare. If you have a particular medical problem, please consult a doctor or a specialist.

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

APP SECURITY SCORE	RISK
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.