# MOBSF

# ANDROID STATIC ANALYSIS REPORT

## Nepal COVID-19 Surveillance (1.1.1)

| | |
|---|---|
| File Name: | Nepal COVID-19 Surveillance 1.1.1.apk |
| Package Name: | com.iclick.covidnew |
| Average CVSS Score: | 5.7 |
| App Security Score: | 75/100 (LOW RISK) |
| Trackers Detection: | 1/285 |

# FILE INFORMATION

**File Name:** Nepal COVID-19 Surveillance 1.1.1.apk
**Size:** 6.03MB
**MD5:** 5805c62cbaa3829f2b4ee99160b24052
**SHA1:** 3855b2c08fe256475562c1be893c33ef55b10366
**SHA256:** 222f032997c456a671b5a9e20183b52ef21683511728198501f85a99ff0f9be5

# APP INFORMATION

**App Name:** Nepal COVID-19 Surveillance
**Package Name:** com.iclick.covidnew
**Main Activity:** com.iclick.covidnew.MainActivity
**Target SDK:** 28
**Min SDK:** 16
**Max SDK:**
**Android Version Name:** 1.1.1
**Android Version Code:** 6

# APP COMPONENTS

**Activities:** 3
**Services:** 5
**Receivers:** 3
**Providers:** 2
**Exported Activities:** 0
**Exported Services:** 1
**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=np, ST=kathmandu, L=kathmandu, O=biz technologies, OU=biz technologies, CN=prasanna tuladhar
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-02-13 12:22:27+00:00
Valid To: 2046-07-01 12:22:27+00:00
Issuer: C=np, ST=kathmandu, L=kathmandu, O=biz technologies, OU=biz technologies, CN=prasanna tuladhar
Serial Number: 0x320cdec9
Hash Algorithm: sha256
md5: fc33b1dfaea745b28fd121c0ac559f6c
sha1: 522aa1623e4127bbb228e4b62e1cb03f7b2ac83f
sha256: 910f4c9609037826aefec62f69d333ad469e0d1970c3cf3be5a75fc06cefcccf
sha512:

2765a4e641d4bf79ddb5369e02b2361f4c90b8e3a1a25cb89d6e83ce20e9550c2b1da498786b488c703502ff83b83a1a6b59f0468f6084cb66693de732852416

PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: f20848dd914e25829265f15074c17f86918782041d246b7fb0df234d351bdec2

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.FOREGROUND_SERVICE | normal | | Allows a regular application to use Service.startForeground |
| 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.WAKE_LOCK | dangerous | prevent phone from sleeping | Allows an application to prevent the phone from going to sleep. |
| android.permission.ACCESS_NETWORK_STATE | normal | view network status | Allows an application to view the status of all networks. |
| 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. |
| com.google.android.c2dm.permission.RECEIVE | signature | C2DM permissions | Permission for cloud to device messaging. |
| com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE | dangerous | Unknown permission from android reference | Unknown permission from android reference |

# APKID ANALYSIS

<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<br>possible Build.SERIAL check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

# MANIFEST ANALYSIS

| ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|
| App has a Network Security Configuration [android:networkSecurityConfig] | info | The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app. |
| Service (io.invertase.firebase.messaging.RNFirebaseMessagingService) is not Protected.<br>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.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked.<br>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.<br>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 |
| --- | --- | --- | --- |
| The App logs information. Sensitive information should never be logged. | info | CVSS V2: 7.5 (high)<br>CWE: CWE-532 - Insertion of Sensitive Information into Log File<br>OWASP MASVS: MSTG-STORAGE-3 | io/invertase/firebase/RNFirebaseModule.java<br>io/invertase/firebase/Utils.java<br>io/invertase/firebase/database/RNFirebaseDatabaseReference.java<br>io/invertase/firebase/database/RNFirebaseDatabase.java<br>io/invertase/firebase/database/RNFirebaseDatabaseUtils.java<br>io/invertase/firebase/instanceid/RNFirebaseInstanceId.java<br>io/invertase/firebase/firestore/RNFirebaseFirestore.java<br>io/invertase/firebase/firestore/FirestoreSerialize.java<br>io/invertase/firebase/firestore/RNFirebaseFirestoreDocumentReference.java<br>io/invertase/firebase/firestore/RNFirebaseFirestoreCollectionReference.java<br>io/invertase/firebase/config/RNFirebaseRemoteConfig.java<br>io/invertase/firebase/auth/RNFirebaseAuth.java<br>io/invertase/firebase/admob/RNFirebaseAdMob.java<br>io/invertase/firebase/storage/RNFirebaseStorage.java<br>io/invertase/firebase/links/RNFirebaseLinks.java<br>io/invertase/firebase/functions/RNFirebaseFunctions.java<br>io/invertase/firebase/fabric/crashlytics/RNFirebaseCrashlytics.java<br>io/invertase/firebase/perf/RNFirebasePerformance.java<br>io/invertase/firebase/messaging/RNFirebaseMessaging.java<br>io/invertase/firebase/messaging/RNFirebaseMessagingService.java<br>io/invertase/firebase/notifications/RNFirebaseNotifications.java<br>io/invertase/firebase/notifications/RNFirebaseNotificationManager.java<br>io/invertase/firebase/notifications/RNFirebaseNotificationsRebootReceiver.java<br>io/invertase/firebase/notifications/DisplayNotificationTask.java<br>io/invertase/firebase/analytics/RNFirebaseAnalytics.java<br>com/horcrux/svg/RadialGradientView.java<br>com/horcrux/svg/VirtualView.java<br>com/horcrux/svg/ImageView.java<br>com/horcrux/svg/UseView.java<br>com/horcrux/svg/MaskView.java<br>com/horcrux/svg/LinearGradientView.java<br>com/horcrux/svg/Brush.java<br>com/horcrux/svg/PatternView.java<br>com/horcrux/svg/ClipPathView.java<br>com/reactnativecommunity/webview/RNCWebViewModule.java<br>com/reactnativecommunity/webview/RNCWebVi |

| ISSUE | SEVERITY | STANDARDS | FILES |
| --- | --- | --- | --- |
| | | | ewManager.java<br>com/swmansion/reanimated/nodes/DebugNode.java<br>com/swmansion/gesturehandler/react/RNGestureHandlerRootHelper.java<br>com/github/mikephil/charting/renderer/ScatterChartRenderer.java<br>com/github/mikephil/charting/renderer/CombinedChartRenderer.java<br>com/github/mikephil/charting/listener/BarLineChartTouchListener.java<br>com/github/mikephil/charting/charts/BarChart.java<br>com/github/mikephil/charting/charts/CombinedChart.java<br>com/github/mikephil/charting/charts/Chart.java<br>com/github/mikephil/charting/charts/HorizontalBarChart.java<br>com/github/mikephil/charting/charts/PieRadarChartBase.java<br>com/github/mikephil/charting/charts/BarLineChartBase.java<br>com/github/mikephil/charting/utils/FileUtils.java<br>com/github/mikephil/charting/utils/Utils.java<br>com/github/mikephil/charting/components/AxisBase.java<br>com/github/mikephil/charting/data/ChartData.java<br>com/github/mikephil/charting/data/PieEntry.java<br>com/github/mikephil/charting/data/LineDataSet.java<br>com/github/mikephil/charting/data/CombinedData.java<br>com/agontuk/RNFusedLocation/RNFusedLocationModule.java<br>com/agontuk/RNFusedLocation/SingleLocationUpdate.java |

| 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)<br>**CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm<br>**OWASP MASVS:** MSTG-CRYPTO-4 | io/invertase/firebase/Utils.java<br>io/invertase/firebase/database/RNFirebaseDatabaseReference.java<br>io/invertase/firebase/database/RNFirebaseDatabase.java<br>io/invertase/firebase/database/RNFirebaseDatabaseUtils.java<br>io/invertase/firebase/firestore/RNFirebaseFirestore.java<br>io/invertase/firebase/firestore/RNFirebaseFirestoreCollectionReference.java<br>io/invertase/firebase/auth/RNFirebaseAuth.java<br>io/invertase/firebase/admob/RNFirebaseAdMobUtils.java<br>io/invertase/firebase/perf/RNFirebasePerformance.java<br>io/invertase/firebase/notifications/RNFirebaseNotificationManager.java<br>io/invertase/firebase/notifications/DisplayNotificationTask.java<br>com/horcrux/svg/PropHelper.java<br>com/horcrux/svg/TSpanView.java<br>com/horcrux/svg/SVGLength.java<br>com/oblador/vectoricons/VectorIconsModule.java<br>com/reactnativecommunity/webview/RNCWebViewManager.java<br>com/github/wuxudong/rncharts/utils/EasingFunctionHelper.java<br>com/github/wuxudong/rncharts/utils/ChartDataSetConfigUtils.java |
| Files may contain hardcoded sensitive informations like usernames, passwords, keys etc. | high | **CVSS V2:** 7.4 (high)<br>**CWE:** CWE-312 - Cleartext Storage of Sensitive Information<br>**OWASP Top 10:** M9: Reverse Engineering<br>**OWASP MASVS:** MSTG-STORAGE-14 | io/invertase/firebase/functions/RNFirebaseFunctions.java<br>io/invertase/firebase/notifications/RNFirebaseNotifications.java<br>io/invertase/firebase/notifications/RNFirebaseNotificationManager.java |

## DOMAIN MALWARE CHECK

| DOMAIN | STATUS | GEOLOCATION |
| --- | --- | --- |
| covid-19-5849f.firebaseio.com | good | **IP:** 35.201.97.85<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |

## URLS

| URL | FILE |
| --- | --- |
| https://covid-19-5849f.firebaseio.com | Android String Resource |

# FIREBASE DATABASES

| FIREBASE URL | DETAILS |
| --- | --- |
| https://covid-19-5849f.firebaseio.com | info<br>App talks to a Firebase Database. |

# TRACKERS

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

# PLAYSTORE INFORMATION

**Title:** Nepal COVID-19 Surveillance

**Score:** 3.825 **Installs:** 5,000+ **Price:** 0 **Android Version Support:** 4.1 and up **Category:** Health & Fitness **Play Store URL:** com.iclick.covidnew

**Developer Details:** iClick, iClick, J.P. Marg, Thamel, Kathmandu, Nepal, http://kathmandu.gov.np, hello.iclick@gmail.com,

**Release Date:** Apr 2, 2020 **Privacy Policy:** Privacy link

**Description:**

Nepal COVID-19 Surveillance System is a collaborative effort of Nepal Research and Education Network (NREN), Center for Information and Communication Technology (ICT4D), Innovative Solution Pvt. Ltd. (Insol), I. Click Pvt. Ltd. (iClick), Public Health Concern Trust-Nepal (PHECT-Nepal), Nepal Disaster and Emergency Medicine Center (NADEM) and Innovative Data Solution Pvt. Ltd. (IDS). The system is designed to detect community spread of the disease, which will help Government, Local Government and Communities to fight against Corona outbreak. Nepal COVID-19 Surveillance System is an Information Technology based Surveillance System which provides mobile app for self-assessment to know how likely he/she is infected by Corona Virus. The system suggests person to go for self-quarantine and ask updating his/her health status continuously for 14 days. The system provides dashboard for medical doctor / health worker to monitor the health status of a person under self-quarantine and registered into the system. The GIS-based mapping capacity of the system helps service providers to track the person in self-quarantine and delivering service at his/her door. Location based system helps decision makers, disaster management team for strategic planning and making decisions to address the issues on real time. Mobile application for self-assessment of possible infection of Corona Virus is the key component of the system, the assessment result provided by the system is mainly depends upon the decision rule deployed in the system. Our collaborating team has deployed "Emergency Healthcare COVID-19 Triage Scale", prepared by Dr. Ramesh Kumar Maharjan, MD, DM EM, Emergency Physician & Dr. Rashmisha Maharjan, MBBS based on data of "25 International Expert WHO Team Finding of Covid-19 Symptoms in China". The system has been adopted by Kathmandu Metropolitan City to provide service to its citizens.

## 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.