ANDROID STATIC ANALYSIS REPORT

Hamro Swasthya (हाम्रो स्वास्थ्य) (1.3.2)

File Name:	Hamro Swasthya (हाम्रो स्वास्थ्य) 1.3.2.apk
Package Name:	np.com.naxa.covid19
Average CVSS Score:	5.2
App Security Score:	75/100 (LOW RISK)

FILE INFORMATION

File Name: Hamro Swasthya (हाम्रो स्वास्थ्य) 1.3.2.apk
Size: 2.25MB
MD5: d05ed0590b9af6b91ecb91a2d38754e9
SHA1: 0f643f599ddf754f4183a039e2bfa6b4ec8708b9
SHA256: eda9fc3c2e361d5a75300894bed99af4b4e2810cf0246e7ce740ee69a84536c1

APP INFORMATION

App Name: Hamro Swasthya (हाम्रो स्वास्थ्य)
Package Name: np.com.naxa.covid19
Main Activity: np.com.naxa.openspaces.MainActivity
Target SDK: 28
Min SDK: 16
Max SDK:
Android Version Name: 1.3.2
Android Version Code: 132

APP COMPONENTS

Activities: 3
Services: 5
Receivers: 2
Providers: 1
Exported Activities: 0
Exported Services: 1
Exported Receivers: 1
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: 2020-03-27 04:49:06+00:00
Valid To: 2050-03-27 04:49:06+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xe3c17a5e7b38b1bcda2fcafa4e8465fa4f32563b
Hash Algorithm: sha256
md5: 8b4f306b4657528c2b13babe3e9bfd65
sha1: e44c0ff1ab06da5a54c6a6939ffb9109a5bca38a
sha256: 3d5864205f3c9f9408a4289969027a69e87adffb2c60a713c08613c9c9d384e5
sha512:
c93aaa397b15dd28ffed2b1595b1a249b7aab646a517dd7f36a211b98233b4d9b79c68773fa22da9f9dda84b3b6aab7ecf884bc265bc3b51d65996b1599980bc

PublicKey Algorithm: rsa
Bit Size: 4096
```

Fingerprint: a9d29af7aaa0718a0ef7986173b8e8cc1d6b7e25bf348648b89c84ddb04180be

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.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.

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
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD 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] flag is missing.	medium	The flag [android:allowBackup] should be set to false. By default it is set to true and 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 (io.flutter.plugins.firebasemessaging.FlutterFirebaseMessagingService) 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.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

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	io/flutter/plugins/urllauncher/c.java io/flutter/plugins/urllauncher/a.java io/flutter/plugins/firebasemessaging/FlutterFirebaseMessagingService.java io/flutter/plugins/firebasemessaging/a.java io/flutter/embedding/engine/f/a.java io/flutter/plugin/platform/i.java io/flutter/plugin/platform/SingleViewPresentation.java io/flutter/view/c.java io/flutter/view/e.java io/flutter/view/g.java io/flutter/view/AccessibilityViewEmbedder.java f/a/a.java f/a/d/a/c.java f/a/d/a/j.java f/a/d/a/a.java c/i/a/c.java c/i/a/d.java c/f/a/a/i/t/a.java c/f/a/b/f/a.java c/f/a/b/d/c/l.java c/f/a/b/d/d/s.java c/f/a/b/e/b/a.java c/f/a/b/b/o.java c/f/a/b/b/h.java c/f/a/b/b/d.java c/f/a/b/b/p.java c/f/a/b/b/g.java c/f/b/c.java c/h/a/c.java c/h/a/d.java c/h/a/a.java b/g/a/a.java b/f/a/b.java b/c/i/b.java b/c/f/a.java b/c/h/b.java b/c/j/b.java b/c/j/c.java b/d/a/b.java b/d/a/e.java b/d/a/j.java b/d/a/m.java b/d/a/a.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) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP MASVS:** MSTG-CRYPTO-4	io/flutter/plugins/urllauncher/a.java io/flutter/plugins/firebase/firebaseremoteconfig/b.java io/flutter/plugins/c/a.java io/flutter/plugins/d/a.java io/flutter/embedding/engine/i/j.java io/flutter/embedding/engine/i/f.java io/flutter/embedding/engine/i/g.java io/flutter/embedding/engine/i/a.java io/flutter/embedding/engine/e/a.java io/flutter/plugin/platform/SingleViewPresentation.java io/flutter/view/AccessibilityViewEmbedder.java i/a/a/a/h.java f/b/a/a/a/a.java h/b.java c/i/a/c.java c/i/a/d.java c/a/a/a.java c/f/a/a/b.java c/f/a/a/a.java c/f/a/a/i/b.java c/f/a/a/i/c.java c/f/a/a/i/g.java c/f/a/a/i/a.java c/f/a/a/i/v/j/b.java c/f/a/b/d/d/g0.java c/f/a/b/d/d/v.java c/f/c/n.java c/f/c/o.java c/f/c/q.java c/f/c/i.java c/f/c/z/a.java c/f/c/y/b.java c/f/c/y/h.java c/f/c/y/g.java c/f/d/c.java c/f/d/h.java c/f/d/i.java c/f/d/s.java c/f/d/l.java c/f/b/c.java c/f/b/m/a.java c/h/a/c.java c/c/a/b.java c/b/a/c.java b/a/a/b/b.java b/c/j/e/b.java b/d/a/d.java b/b/b.java b/b/d.java b/b/e.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	io/flutter/plugin/platform/c.java

ISSUE	SEVERITY	STANDARDS	FILES
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	c/i/a/c.java c/f/a/a/i/v/j/z.java c/f/a/a/i/v/j/e0.java c/f/a/a/i/v/j/d0.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
github.com	good	**IP:** 13.237.44.5 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map
covid19-dev-1125e.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/flutter/flutter/issues/2897).It	io/flutter/plugin/platform/i.java
https://covid19-dev-1125e.firebaseio.com	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://covid19-dev-1125e.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	c/f/a/b/b/u.java

PLAYSTORE INFORMATION

Title: Hamro Swasthya

Score: 4.31 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** 4.1 and up **Category:** Health & Fitness **Play Store URL:** np.com.naxa.covid19

Developer Details: Ministry of Health and Population, Ministry+of+Health+and+Population, None, http://www.mohp.gov.np, itsec@mohp.gov.np,

Release Date: Mar 30, 2020 **Privacy Policy:** Privacy link

Description:

Hamro Swasthya is a mobile application developed by Ministry of Health and Population, Government of Nepal to provide reliable information on important health to Nepali citizens. At this time of COVID-19 global pandemic, this app is dedicated towards COVID-19 control and awareness, but the overall target of the application is to cover all health related issues in coming days.

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.