ANDROID STATIC ANALYSIS REPORT

Care Workforce (5.13.21)

File Name:	Care Workforce_com.hivelearning.nhsc.apk
Package Name:	com.hivelearning.nhsc
Average CVSS Score:	5.9
App Security Score:	20/100 (HIGH RISK)
Trackers Detection:	2/285

FILE INFORMATION

File Name: Care Workforce_com.hivelearning.nhsc.apk
Size: 67.82MB
MD5: baa13d675b0d1ee09068212925ae3e42
SHA1: 1332be371a3fb526a2e65006b089569274f02269
SHA256: fb34fd3cd74008835aeea98a8a1e4ce3e70d8154511f68d5e356787c07cbc80a

APP INFORMATION

App Name: Care Workforce
Package Name: com.hivelearning.nhsc
Main Activity: com.hiveapp.SplashActivity
Target SDK: 28
Min SDK: 16
Max SDK:
Android Version Name: 5.13.21
Android Version Code: 1449

APP COMPONENTS

Activities: 7
Services: 8
Receivers: 7
Providers: 4
Exported Activities: 2
Exported Services: 2
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
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: 2018-05-04 09:39:40+00:00
Valid To: 2048-05-04 09:39:40+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xf22dd3ef09886454f15104840859b8717a91c228
Hash Algorithm: sha256
md5: c0774209e5585c5346d74d29be64016b
sha1: 5d3b809883c54cced91e445f78dec94245041fa9
sha256: 578d6854db5a966eb8da7c5e886e6a6023ff821b1eaff36f50b93daeae74d2b2
sha512:
594baef74d219019eea3879da8614a2212c186ed2cf5d51007e2a23261a4a9b752702073bb47a8cd3ad6a40503f1ab3263d1c23bb56fd2dbc8a7534f0fc849a2

PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 8e73a55040316df37d5d9e91cde6f671beae9709967841f1ccfb937fb2a1c670

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.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
android.permission.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
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
com.android.vending.CHECK_LICENSE	dangerous	Unknown permission from android reference	Unknown permission from android reference
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read SD card contents	Allows an application to read from SD Card.

SHARED LIBRARY BINARY ANALYSIS

ISSUE	SEVERITY	DESCRIPTION	FILES
Found elf built without Position Independent Executable (PIE) flag	high	In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, Address space layout randomization (ASLR) randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack, heap and libraries. Built with option -pie.	lib/mips64/libmodft2.so lib/mips64/libc++_shared.so lib/mips64/libmodpdfium.so lib/mips64/libmodpng.so lib/mips64/libjniPdfium.so

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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
network operator name 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>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.hiveapp.MainActivity	Schemes: https://, v3hiveapp://, Hosts: workforce.adultsocialcare.uk, v3auth, *.morehive.com, *.hivelearning.com,
net.openid.appauth.RedirectUriReceiverActivity	Schemes: hiveapp://,

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
Broadcast Receiver (io.invertase.firebase.notifications.RNFirebaseNotificationsRebootReceiver) is not Protected. [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.
Service (io.invertase.firebase.messaging.RNFirebaseMessagingService) 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.

ISSUE	SEVERITY	DESCRIPTION
Service (io.invertase.firebase.messaging.RNFirebaseInstanceIdService) 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.
Launch Mode of Activity (com.hiveapp.MainActivity) 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.hiveapp.MainActivity) 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.
Launch Mode of Activity (net.openid.appauth.AuthorizationManagementActivity) 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 (net.openid.appauth.RedirectUriReceiverActivity) 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.
Broadcast Receiver (com.learnium.RNDeviceInfo.RNDeviceReceiver) is not Protected. [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.
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.

ISSUE	SEVERITY	DESCRIPTION
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
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	org/greenrobot/eventbus/Subscription.java org/greenrobot/eventbus/SubscriberMethod.java io/invertase/firebase/Utils.java io/invertase/firebase/firestore/RNFirebaseFirestore.java io/invertase/firebase/firestore/RNFirebaseFirestoreCollectionReference.java io/invertase/firebase/auth/RNFirebaseAuth.java io/invertase/firebase/database/RNFirebaseDatabaseReference.java io/invertase/firebase/database/RNFirebaseDatabase.java io/invertase/firebase/database/RNFirebaseDatabaseUtils.java io/invertase/firebase/perf/RNFirebasePerformance.java io/invertase/firebase/admob/RNFirebaseAdMobUtils.java io/invertase/firebase/notifications/DisplayNotificationTask.java io/invertase/firebase/notifications/RNFirebaseNotificationManager.java net/openid/appauth/AuthState.java net/openid/appauth/browser/BrowserDescriptor.java com/imagepicker/utils/UI.java com/reactnativecommunity/webview/RNCWebViewManager.java com/proyecto26/inappbrowser/ChromeTabsManagerActivity.java com/bugsnag/BugsnagReactNative.java com/bugsnag/DiagnosticsCallback.java com/bugsnag/android/HandledState.java com/bugsnag/android/ErrorReader.java com/bugsnag/android/Severity.java com/horcrux/svg/SVGLength.java com/horcrux/svg/PropHelper.java com/horcrux/svg/TSpanView.java com/oblador/vectoricons/VectorIconsModule.java com/RNFetchBlob/RNFetchBlobFS.java
			org/greenrobot/eventbus/EventBus.java org/greenrobot/eventbus/BackgroundPoster.java org/greenrobot/eventbus/util/ExceptionToResourceMapping.java org/greenrobot/eventbus/util/ErrorDialogManager.java org/greenrobot/eventbus/util/AsyncExecutor.java org/greenrobot/eventbus/util/ErrorDialogConfig.java org/wonday/pdf/PdfView.java io/invertase/firebase/Utils.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	io/invertase/firebase/RNFirebaseModule.java io/invertase/firebase/messaging/RNFirebaseMessaging.java io/invertase/firebase/messaging/RNFirebaseMessagingService.java io/invertase/firebase/firestore/RNFirebaseFirestore.java io/invertase/firebase/firestore/FirestoreSerialize.java io/invertase/firebase/firestore/RNFirebaseFirestoreCollectionReference.java io/invertase/firebase/firestore/RNFirebaseFirestoreDocumentReference.java io/invertase/firebase/auth/RNFirebaseAuth.java io/invertase/firebase/database/RNFirebaseDatabaseReference.java io/invertase/firebase/database/RNFirebaseDatabase.java io/invertase/firebase/database/RNFirebaseDatabaseUtils.java io/invertase/firebase/perf/RNFirebasePerformance.java io/invertase/firebase/functions/RNFirebaseFunctions.java io/invertase/firebase/fabric/crashlytics/RNFirebaseCrashlytics.java io/invertase/firebase/storage/RNFirebaseStorage.java io/invertase/firebase/admob/RNFirebaseAdMob.java io/invertase/firebase/config/RNFirebaseRemoteConfig.java io/invertase/firebase/instanceid/RNFirebaseInstanceId.java io/invertase/firebase/analytics/RNFirebaseAnalytics.java io/invertase/firebase/notifications/RNFirebaseNotifications.java io/invertase/firebase/notifications/RNFirebaseNotificationsRebootReceiver.java io/invertase/firebase/notifications/DisplayNotificationTask.java io/invertase/firebase/notifications/RNFirebaseNotificationManager.java io/invertase/firebase/links/RNFirebaseLinks.java net/openid/appauth/internal/Logger.java com/imagepicker/utils/MediaUtils.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/reactnativecommunity/webview/RNCWebViewManager.java com/reactnativecommunity/webview/RNCWebViewModule.java com/lugg/ReactNativeConfig/ReactNativeConfigModule.java com/bugsnag/android/Logger.java com/bugsnag/android/ExceptionHandler.java com/bugsnag/android/ndk/NativeBrid

ISSUE	SEVERITY	STANDARDS	FILES
			ge.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java com/shockwave/pdfium/PdfiumCore.java com/horcrux/svg/UseView.java com/horcrux/svg/RadialGradientView.java com/horcrux/svg/VirtualView.java com/horcrux/svg/LinearGradientView.java com/horcrux/svg/Brush.java com/horcrux/svg/MaskView.java com/horcrux/svg/ClipPathView.java com/horcrux/svg/ImageView.java com/horcrux/svg/PatternView.java com/brentvatne/react/ReactVideoView.java com/github/barteksc/pdfviewer/RenderingHandler.java com/github/barteksc/pdfviewer/PDFView.java com/github/barteksc/pdfviewer/link/DefaultLinkHandler.java com/github/yamill/orientation/OrientationModule.java com/oblador/keychain/KeychainModule.java com/oblador/keychain/cipherStorage/CipherStorageKeystoreAESCBC.java com/rnappauth/utils/UnsafeConnectionBuilder.java com/RNFetchBlob/RNFetchBlobReq.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/invertase/firebase/functions/RNFirebaseFunctions.java io/invertase/firebase/notifications/RNFirebaseNotifications.java io/invertase/firebase/notifications/RNFirebaseNotificationManager.java net/openid/appauth/ClientSecretPost.java net/openid/appauth/TokenRequest.java net/openid/appauth/RegistrationResponse.java com/bugsnag/android/Breadcrumb.java com/bugsnag/android/EventReceiver.java com/bugsnag/android/Client.java com/bugsnag/android/Configuration.java com/bugsnag/android/ConfigFactory.java com/bugsnag/android/DeviceData.java com/bugsnag/android/ExceptionHandler.java com/hiveapp/BuildConfig.java

ISSUE	SEVERITY	STANDARDS	FILES
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	io/invertase/firebase/storage/RNFirebaseStorage.java com/imagepicker/utils/MediaUtils.java com/imagepicker/utils/RealPathUtil.java com/reactnativecommunity/webview/RNCWebViewModule.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/RNFetchBlob/RNFetchBlobFS.java com/RNFetchBlob/Utils/PathResolver.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/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.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/reactnativecommunity/webview/RNCWebViewModule.java com/RNFetchBlob/RNFetchBlobBody.java
This App may have root detection capabilities.	secure	**CVSS V2:** 0 (info) **OWASP MASVS:** MSTG-RESILIENCE-1	com/bugsnag/android/DeviceData.java
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	com/RNFetchBlob/RNFetchBlobUtils.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
graphql.hivelearning.com	good	**IP:** 35.177.249.166 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.50853 **Longitude:** -0.12574 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.hivelearning.com	good	**IP:** 13.224.239.11 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.50853 **Longitude:** -0.12574 **View:** Google Map
auth.hivelearning.com	good	**IP:** 18.132.116.180 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
nhs-care.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
cdn2.hivelearning.com	good	**IP:** 52.85.104.34 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.714272 **Longitude:** -74.005966 **View:** Google Map
notify.bugsnag.com	good	**IP:** 35.186.205.6 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
bugsnag.com	good	**IP:** 13.224.239.57 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.50853 **Longitude:** -0.12574 **View:** Google Map
api.hivelearning.io	good	**IP:** 52.84.94.100 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
m4vum4t128.execute-api.eu-west-2.amazonaws.com	good	**IP:** 52.85.104.41 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.714272 **Longitude:** -74.005966 **View:** Google Map
sessions.bugsnag.com	good	**IP:** 35.190.88.7 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.example.com	good	**IP:** 93.184.216.34 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.04372 **Longitude:** -77.487488 **View:** Google Map
github.com	good	**IP:** 140.82.118.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.7757 **Longitude:** -122.395203 **View:** Google Map

URLS

URL	FILE
http://www.example.com	net/openid/appauth/browser/BrowserSelector.java
https://github.com/bugsnag/bugsnag-react-native	com/bugsnag/DiagnosticsCallback.java
https://notify.bugsnag.com https://sessions.bugsnag.com	com/bugsnag/android/Configuration.java
https://bugsnag.com	com/bugsnag/android/Notifier.java
https://api.hivelearning.io https://auth.hivelearning.com https://cdn2.hivelearning.com https://graphql.hivelearning.com https://m4vum4t128.execute-api.eu-west-2.amazonaws.com/prod www.hivelearning.com	com/hiveapp/BuildConfig.java

URL	FILE
https://api.hivelearning.io https://auth.hivelearning.com https://cdn2.hivelearning.com https://graphql.hivelearning.com https://m4vum4t128.execute-api.eu-west-2.amazonaws.com/prod www.hivelearning.com https://nhs-care.firebaseio.com	Android String Resource

FIREBASE DATABASES

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

TRACKERS

TRACKER	URL
Bugsnag	https://reports.exodus-privacy.eu.org/trackers/207
Google Firebase Analytics	https://reports.exodus-privacy.eu.org/trackers/49

PLAYSTORE INFORMATION

Title: Care Workforce

Score: 0.0 **Installs:** 5,000+ **Price:** 0 **Android Version Support:** 4.1 and up **Category:** Productivity **Play Store URL:** com.hivelearning.nhsc

Developer Details: Hive Learning, Hive+Learning, None, http://www.hivelearning.com/site, help@hivelearning.com,

Release Date: May 1, 2020 **Privacy Policy:** Privacy link

Description:

Join the Official Department of Health and Social Care COVID-19 Workforce app to: Get up-to-the-minute advice on everything you need to know about managing Covid-19 – all in one easy-to-access digital hub. Practical resources on everything from daily briefings, to the latest on safety and procedural advice, offers for NHS staff, wellbeing tips, and more. All the information you need in one place – access from any device with the internet so you can easily search and get trusted information fast. Instant notifications in your inbox and on your phone to keep you up to date with the latest info the moment it's released.

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 v3.0.9 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.