ANDROID STATIC ANALYSIS REPORT

Carteira de Trabalho Digital (5.4.5)

File Name:	mindotrabalho.apk
Package Name:	br.gov.dataprev.carteiradigital
Scan Date:	June 20, 2023, 9:02 p.m.
App Security Score:	47/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	3/428

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	16	3	0	1

FILE INFORMATION

File Name: mindotrabalho.apk
Size: 13.17MB
MD5: ca609a265a143de3a7e90b3e04235e9c
SHA1: 783842feda0163e685d8ca0338221f59fdefa40c
SHA256: 411a27d5241f6e6c7a18a31c86a7440427304202727a4b9a68634053f1f3f266

APP INFORMATION

App Name: Carteira de Trabalho Digital
Package Name: br.gov.dataprev.carteiradigital
Main Activity: br.gov.dataprev.carteiradigital.MainActivity
Target SDK: 33
Min SDK: 21

Max SDK:
Android Version Name: 5.4.5
Android Version Code: 516

APP COMPONENTS

Activities: 6
Services: 15
Receivers: 16
Providers: 10
Exported Activities: 1
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=BR, ST=RJ, L=Rio de Janeiro, O=DATAPREV, OU=SUDS, CN=Diogo Costa Martins Pizaneschi
Signature Algorithm: dsa
Valid From: 2017-04-03 21:03:26+00:00
Valid To: 2044-08-19 21:03:26+00:00
Issuer: C=BR, ST=RJ, L=Rio de Janeiro, O=DATAPREV, OU=SUDS, CN=Diogo Costa Martins Pizaneschi
Serial Number: 0x724cc316
Hash Algorithm: sha1
md5: 6cc50dd9fcacded7d31b289266ada574
sha1: c57c25b8274a37e4c4d03cfa6720a224d0071811
sha256: a0bdad858292a7bc69d46b4057d90c48ccc99e9519559714cf607ce92ccefa54
sha512: aa60c33f129a7288c3bbe0497a08fc303e6ba2fa4dd829630a77382b80b9bb2fc203e379644600b12aecae96b229bf712736eae95a4b61b7ca0cfafc30c85600
PublicKey Algorithm: dsa
Bit Size: 1024
```

Fingerprint: 9af32ba3ea64cf0f70a86ce1cf1770c69ba7fd18f0b3934aa74aad740317ce23

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_MEDIA_IMAGES	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.USE_BIOMETRIC	normal		Allows an app to use device supported biometric modalities.

PERMISSION	STATUS	INFO	DESCRIPTION
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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.POST_NOTIFICATIONS	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.google.android.gms.permission.AD_ID	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_FULL_SCREEN_INTENT	normal		Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.SCHEDULE_EXACT_ALARM	normal		Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.BROADCAST_CLOSE_SYSTEM_DIALOGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NOTIFICATION_POLICY	normal		Marker permission for applications that wish to access notification policy.

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.MANUFACTURER check
possible Build.SERIAL check
Build.TAGS check
SIM operator check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

FILE	FINDINGS	DETAILS
classes2.dex	Anti-VM Code	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
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)
classes3.dex	Anti-VM Code	Build.FINGERPRINT check possible Build.SERIAL check
	Compiler	r8 without marker (suspicious)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
br.gov.dataprev.carteiradigital.MainActivity	Schemes: ectpsmobile://,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **2** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **6** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=21]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 to receive reasonable security updates.
2	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.
3	Broadcast Receiver (io.invertase.firebase.messaging.ReactNativeFirebaseMessagingReceiver) 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]	warning	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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	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.
5	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	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.
6	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]	warning	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.

NO	ISSUE	SEVERITY	DESCRIPTION
7	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]	warning	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.

CODE ANALYSIS

HIGH: **0** | WARNING: **6** | INFO: **3** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				app/notifee/core/AlarmPermissionBroadcastReceiver.java app/notifee/core/Logger.java app/notifee/core/RebootBroadcastReceiver.java app/notifee/core/b.java cl/json/RNShareModule.java cl/json/social/InstagramShare.java cl/json/social/SingleShareIntent.java com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java com/appdynamics/eum/reactnative/ReactNativeAppdynamicsModule.java com/appdynamics/eumagent/runtime/Instrumentation.java com/appdynamics/eumagent/runtime/logging/ADLog.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/appdynamics/eumagent/runtime/p000private/ad.java com/appdynamics/eumagent/runtime/p000private/ak.java com/appdynamics/eumagent/runtime/p000private/an.java com/appdynamics/eumagent/runtime/p000private/az.java com/appdynamics/eumagent/runtime/p000private/ba.java com/appdynamics/eumagent/runtime/p000private/bm.java com/appdynamics/eumagent/runtime/p000private/bp.java com/appdynamics/eumagent/runtime/p000private/bv.java com/appdynamics/eumagent/runtime/p000private/cg.java com/appdynamics/eumagent/runtime/p000private/e.java com/appdynamics/eumagent/runtime/p000private/k.java com/appdynamics/eumagent/runtime/p000private/u.java com/appdynamics/eumagent/runtime/p000private/x.java com/github/barteksc/pdfviewer/PDFView.java com/github/barteksc/pdfviewer/RenderingHandler.java com/github/barteksc/pdfviewer/link/DefaultLinkHandler.java com/horcrux/svg/Brush.java com/horcrux/svg/ClipPathView.java com/horcrux/svg/ImageView.java com/horcrux/svg/LinearGradientView.java com/horcrux/svg/PatternView.java com/horcrux/svg/RadialGradientView.java com/horcrux/svg/UseView.java com/horcrux/svg/VirtualView.java com/ibits/react_native_in_app_review/AppReviewModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/imagepicker/ImageMetadata.java com/imagepicker/Metadata.java com/imagepicker/VideoMetadata.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/RNInstallReferrerClient.java com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java com/lugg/RNCConfig/RNCConfigModule.java com/oblador/keychain/KeychainModule.java com/oblador/keychain/cipherStorage/CipherStorageBase.java com/oblador/keychain/cipherStorage/CipherStorageFacebookConceal.java com/oblador/keychain/cipherStorage/CipherStorageKeystoreAesCbc.java com/oblador/keychain/cipherStorage/CipherStorageKeystoreRsaEcb.java com/oblador/keychain/decryptionHandler/DecryptionResultHandlerInteractiveBiometric.java com/oblador/keychain/decryptionHandler/DecryptionResultHandlerInteractiveBiometricManualRetry.java com/proyecto26/inappbrowser/RNInAppBrowser.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/reactnativecommunity/webview/RNCWebViewManager.java com/reactnativedocumentpicker/DocumentPickerModule.java com/reactnativeimageresizer/ImageResizer.java com/reactnativeimageresizer/ImageResizerModuleImpl.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/shockwave/pdfium/PdfiumCore.java com/swmansion/reanimated/NativeMethodsHelper.java com/swmansion/reanimated/NativeProxy.java com/swmansion/reanimated/ReanimatedJSIModulePackage.java com/swmansion/reanimated/ReanimatedModule.java com/swmansion/reanimated/layoutReanimation/AnimationsManager.java com/swmansion/reanimated/layoutReanimation/ReanimatedNativeHierarchyManager.java com/swmansion/reanimated/nodes/DebugNode.java com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/th3rdwave/safeareacontext/SafeAreaView.java com/zoontek/rnbootsplash/RNBootSplashModule.java io/invertase/firebase/app/ReactNativeFirebaseApp.java io/invertase/firebase/common/RCTConvertFirebase.java io/invertase/firebase/common/ReactNativeFirebaseEventEmitter.java io/invertase/firebase/common/SharedUtils.java io/invertase/firebase/crashlytics/ReactNativeFirebaseCrashlyticsInitProvider.java io/invertase/firebase/crashlytics/ReactNativeFirebaseCrashlyticsModule.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingModule.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingReceiver.java io/invertase/firebase/perf/ScreenTrace.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/invertase/notifee/NotifeeReactUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/invertase/notifee/NotifeeReactUtils.java net/rhogan/rnsecurerandom/PRNGFixes.java org/wonday/pdf/PdfView.java
2	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/ReactNativeBlobUtil/ReactNativeBlobUtilFS.java com/ReactNativeBlobUtil/Utils/PathResolver.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnativecommunity/webview/RNCWebViewModule.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java
3	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/ReactNativeBlobUtil/ReactNativeBlobUtilBody.java com/reactnativecommunity/webview/RNCWebViewModule.java
4	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/ReactNativeBlobUtil/ReactNativeBlobUtilUtils.java com/appdynamics/eumagent/runtime/p000private/bg.java
5	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.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/appdynamics/eumagent/runtime/p000private/af.java com/appdynamics/eumagent/runtime/p000private/ai.java com/appdynamics/eumagent/runtime/p000private/aj.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	com/reactnativecommunity/clipboard/ClipboardModule.java
7	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/reactnativecommunity/clipboard/ClipboardModule.java
8	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	br/gov/dataprev/carteiradigital/BuildConfig.java com/appdynamics/eumagent/runtime/Instrumentation.java com/oblador/keychain/KeychainModule.java io/invertase/firebase/common/TaskExecutorService.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingHeadlessService.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingSerializer.java io/invertase/notifee/NotifeeEventSubscriber.java
9	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	net/rhogan/rnsecurerandom/PRNGFixes.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application implement DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower.
12	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
13	FCS_COP.1.1(3)	Selection-Based Security Functional Requirements	Cryptographic Operation - Signing	The application perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
14	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
15	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
16	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
17	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
18	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.
19	FCS_CKM.1.1(2)	Optional Security Functional Requirements	Cryptographic Symmetric Key Generation	The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
mobile.eum-appdynamics.com	ok	**IP:** 34.208.171.87 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.gov.br	ok	**IP:** 161.148.164.31 **Country:** Brazil **Region:** Distrito Federal **City:** Brasilia **Latitude:** -15.779720 **Longitude:** -47.929722 **View:** Google Map
www.facebook.com	ok	**IP:** 31.13.90.35 **Country:** United States of America **Region:** Texas **City:** Fort Worth **Latitude:** 32.725410 **Longitude:** -97.320847 **View:** Google Map
mte.api.dataprev.gov.br	ok	**IP:** 200.152.35.66 **Country:** Brazil **Region:** Rio de Janeiro **City:** Rio de Janeiro **Latitude:** -22.902781 **Longitude:** -43.207500 **View:** Google Map
github.com	ok	**IP:** 20.201.28.151 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cidadao.dataprev.gov.br	ok	**IP:** 200.152.32.46 **Country:** Brazil **Region:** Rio de Janeiro **City:** Rio de Janeiro **Latitude:** -22.902781 **Longitude:** -43.207500 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.78.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
notifee.app	ok	**IP:** 52.67.97.86 **Country:** Brazil **Region:** Sao Paulo **City:** Sao Paulo **Latitude:** -23.547501 **Longitude:** -46.636108 **View:** Google Map
play.google.com	ok	**IP:** 142.250.78.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
empregabrasil.mte.gov.br	ok	**IP:** 200.152.40.87 **Country:** Brazil **Region:** Rio de Janeiro **City:** Rio de Janeiro **Latitude:** -22.902781 **Longitude:** -43.207500 **View:** Google Map
pinterest.com	ok	**IP:** 151.101.192.84 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
eum-appd.dataprev.gov.br	ok	**IP:** 200.152.45.55 **Country:** Brazil **Region:** Rio de Janeiro **City:** Rio de Janeiro **Latitude:** -22.902781 **Longitude:** -43.207500 **View:** Google Map
twitter.com	ok	**IP:** 104.244.42.193 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
image.eum-appdynamics.com	ok	**IP:** 35.164.70.124 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
plus.google.com	ok	**IP:** 142.250.78.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
dtp-ectps-digital.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
sso.acesso.gov.br	ok	**IP:** 189.9.113.9 **Country:** Brazil **Region:** Distrito Federal **City:** Brasilia **Latitude:** -15.779720 **Longitude:** -47.929722 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://dtp-ectps-digital.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

TRACKER	CATEGORIES	URL
Appdynamics	Analytics, Profiling	https://reports.exodus-privacy.eu.org/trackers/194
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"APP_DYNAMICS_KEY" : "EUM-AAB-AUS"
"OAUTH_ALLOW_INSECURE_HTTP_REQUESTS" : "false"
"OAUTH_CLIENT_ID" : "ectpsmobile"

POSSIBLE SECRETS
"OAUTH_ISSUER" : ""
"OAUTH_LOGIN_REDIRECT_URI" : "ectpsmobile://loginsuccess"
"OAUTH_LOGOUT_REDIRECT_URI" : "ectpsmobile://logoutsuccesscode"
"OAUTH_SCOPES" : "openid,email,phone,profile,govbr_confiabilidades"
"OAUTH_SERVICE_AUTHORIZATION_ENDPOINT" : "https://sso.acesso.gov.br/authorize"
"OAUTH_SERVICE_END_SESSION_ENDPOINT" : "https://sso.acesso.gov.br/logout"
"OAUTH_SERVICE_TOKEN_ENDPOINT" : "https://mte.api.dataprev.gov.br/apis/ectpsservices/v1/auth/token"
"OAUTH_USE_NONCE" : "true"
"OAUTH_USE_OIDC_DISCOVERY" : "false"
"OAUTH_USE_PKCE" : "true"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"firebase_database_url" : "https://dtp-ectps-digital.firebaseio.com"
"google_api_key" : "AIzaSyDAMhzE9lzvm8EOHT0wsWiGj4rgQrhvdLo"
"google_crash_reporting_api_key" : "AIzaSyDAMhzE9lzvm8EOHT0wsWiGj4rgQrhvdLo"

PLAYSTORE INFORMATION

Title: Carteira de Trabalho Digital

Score: 3.7 **Installs:** 50,000,000+ **Price:** 0 **Android Version Support:** **Category:** Tools **Play Store URL:** br.gov.dataprev.carteiradigital

Developer Details: Serviços e Informações do Brasil, 5829287075355252046, None, https://empregabrasil.mte.gov.br/ , atendimento@dataprev.gov.br,

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

Description:

The Digital Employment Card is a tool for citizens to easily monitor their working life, having access to personal data and their employment contracts that are registered in the Employment and Social Security Card. The Digital Work Card also allows you to apply for Unemployment Insurance, and consult other labor benefits, such as Salary Bonus, TAC-Taxi Driver Benefit and Emergency Benefit.

Report Generated by - MobSF v3.6.7 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.