MOBSF

ANDROID STATIC ANALYSIS REPORT

CSL Plasma (3.42.36)

File Name:	com.cslplasma.cslplasmadonorapplication_1836.apk
Package Name:	com.cslplasma.cslplasmadonorapplication
Scan Date:	Aug. 29, 2025, 9:23 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	17	4	3	1

FILE INFORMATION

File Name: com.cslplasma.cslplasmadonorapplication_1836.apk
Size: 17.58MB
MD5: b34af4eff9259a270987100ed98644c8
SHA1: 3193a4f27aa558954326d8436a1a078eb60bd0f1
SHA256: 8ac86ec8c1ab162f9e386a74e1206c3ec5d2aafb1b7530b26c3908b735a6ab36

APP INFORMATION

App Name: CSL Plasma
Package Name: com.cslplasma.cslplasmadonorapplication
Main Activity: com.cslplasma.cslplasmadonorapplication.MainActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 3.42.36

Android Version Code: 1836

APP COMPONENTS

Activities: 11
Services: 15
Receivers: 7
Providers: 8
Exported Activities: 0
Exported Services: 2
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-03-31 03:37:27+00:00
Valid To: 2050-03-31 03:37:27+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x50cf46ee1fb3c28cff8fd5cf5a9d09e22aeb5f46
Hash Algorithm: sha256
md5: 09045d2e7678789af03f4c1cc95a4824
sha1: 998642803446cf50d99dd369c73723a724154758
sha256: 78d5e71d75432126c7dbe8beaae08f825b61ffda4f356ffc260b0cebc0f3de0f
sha512: 7d7d2066794380f2834fd6187c08010a2b821ca5b852e170a408a42317530748f0df2d7e0758e437f99077159fd5d3101b8199e1348623c05d0df8cfe0a2bc4c
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 354408d9e6188bf84fd31bb89c6c03085250c8480987b0bdff4d4241a4846bc4
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.EXPAND_STATUS_BAR	normal	expand/collapse status bar	Allows application to expand or collapse the status bar.
android.permission.WAKE_LOCK	normal	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_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
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.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.

PERMISSION	STATUS	INFO	DESCRIPTION
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

FILE	DETAILS
b34af4eff9259a270987100ed98644c8.apk	FINDINGS: Anti-VM Code — DETAILS: possible VM check

<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>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></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
SIM operator check
network operator name check
possible VM check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.cslplasma.cslplasmadonorapplication.MainActivity	Schemes: cslplasmaapp://, Hosts: csl.plasma.app, Paths: /app,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 7 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 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.
4	Broadcast Receiver (com.learnium.RNDeviceInfo.RNDeviceReceiver) is not Protected. [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.
5	Service (com.wix.reactnativenotifications.fcm.FcmInstanceIdListenerService) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
6	TaskAffinity is set for activity (com.salesforce.marketingcloud.notifications.NotificationOpenActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
7	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.
8	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: 1 | WARNING: 8 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/d.java a1/g.java a1/n.java b1/h.java b7/a0.java b7/x.java b7/z.java cl/json/RNShareModule.java com/airbnb/android/react/lottie/LottieAnimationViewManager.java com/airbnb/android/react/maps/d.java com/airbnb/android/react/maps/e.java com/brentvatne/react/b.java com/cslplasma/cslplasmadonorapplication/AppEventMoudle.java com/cslplasma/cslplasmadonorapplication/MainApplication.java com/ibits/react_native_in_app_review/AppReviewModule.java com/imagepicker/b.java com/imagepicker/g.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/c.java com/reactnative/ivpusic/imagepicker/a.java com/reactnative/ivpusic/imagepicker/f.java com/reactnativecommunity/asyncstorage/c.java com/reactnativecommunity/webview/e.java com/reactnativecommunity/webview/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/reactnativecommunity/webview/k.java com/rnfs/c.java com/rt2zz/reactnativecontacts/a.java com/salesforce/marketingcloud/MCLogListener.java com/salesforce/marketingcloud/g.java com/salesforce/marketingcloud/tozny/AesCbcWithIntegrity.java com/swmansion/gesturehandler/react/RNGestureHandlerModule.java com/swmansion/gesturehandler/react/j.java com/swmansion/gesturehandler/react/k.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/swmansion/rnscreens/ScreensModule.java com/swmansion/rnscreens/SearchBarManager.java com/th3rdwave/safeareacontext/g.java com/vonovak/AddCalendarEventModule.java com/wix/reactnativenotifications/RNNotificationsModule.java com/yalantis/ucrop/UCropActivity.java com/yalantis/ucrop/task/BitmapCropTask.java com/yalantis/ucrop/view/b.java d0/c.java e3/d.java e6/g.java e8/d.java fr/greweb/reactnativeviewshot/RNViewShotModule.java fr/greweb/reactnativeviewshot/a.java g6/a0.java g6/b.java g6/c.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	g6/d0.java g6/e0.java g6/k.java g6/x.java g6/y.java g9/b.java ge/c.java h6/b0.java h6/e.java h6/g0.java h6/j.java h6/k.java h6/l0.java h6/o.java h6/x.java h7/m0.java h8/g.java h9/c.java io/invertase/firebase/app/a.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingModule.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingReceiver.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java j6/b0.java k/g.java k0/a.java k6/a.java k6/a1.java k6/c.java k6/d0.java k6/d1.java k6/e1.java k6/f1.java k6/g0.java k6/h1.java k6/n1.java k6/r1.java l/c.java l7/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				m8/i.java ma/a.java n0/d.java n1/c.java n5/k.java n6/a.java n7/a.java o0/a.java o6/b.java o7/a.java org/wonday/orientation/a.java p6/f.java p6/m.java p6/n.java p8/e.java q/d.java q1/a.java q5/a.java qe/e.java r/c.java r/k.java r/l.java r1/b.java r7/h.java r9/m.java s0/a.java s6/h.java s8/f.java s8/n.java sa/a.java t/f.java t0/l0.java t6/b.java ta/a.java ta/c.java ta/f.java v/a.java v/b.java v/c.java w2/f.java wa/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				wa/m.java x4/a.java z0/b.java z5/a.java z5/d.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/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnative/ivpusic/imagepicker/a.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/reactnativecommunity/webview/k.java com/rnfs/RNFSManager.java h2/a.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java r1/a.java x1/a.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/airbnb/android/react/maps/AirMapModule.java com/airbnb/android/react/maps/n.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnativecommunity/webview/k.java fr/greweb/reactnativeviewshot/RNViewShotModule.java g9/c.java x1/a.java
				com/reactnativecommunity/asyncstorage/f.java com/salesforce/marketingcloud/storag

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	e/db/a.java com/salesforce/marketingcloud/storage/db/b.java com/salesforce/marketingcloud/storage/db/c.java com/salesforce/marketingcloud/storage/db/e.java com/salesforce/marketingcloud/storage/db/f.java com/salesforce/marketingcloud/storage/db/g.java com/salesforce/marketingcloud/storage/db/h.java com/salesforce/marketingcloud/storage/db/i.java com/salesforce/marketingcloud/storage/db/j.java com/salesforce/marketingcloud/storage/db/k.java com/salesforce/marketingcloud/storage/db/l.java com/salesforce/marketingcloud/storage/db/m.java com/salesforce/marketingcloud/storage/db/upgrades/a.java com/salesforce/marketingcloud/storage/db/upgrades/b.java com/salesforce/marketingcloud/storage/db/upgrades/c.java com/salesforce/marketingcloud/storage/db/upgrades/d.java com/salesforce/marketingcloud/storage/db/upgrades/e.java com/salesforce/marketingcloud/storage/db/upgrades/f.java com/salesforce/marketingcloud/storage/db/upgrades/g.java com/salesforce/marketingcloud/storage/db/upgrades/h.java com/salesforce/marketingcloud/storag

NO	ISSUE	SEVERITY	STANDARDS	FILES
				e/db/upgrades/i.java u5/t0.java u5/t0.java
5	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	com/reactnative/ivpusic/imagepicker/PickerModule.java com/salesforce/marketingcloud/events/f.java com/salesforce/marketingcloud/events/g.java com/salesforce/marketingcloud/registration/Registration.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	pe/c.java pe/d.java pe/i.java pe/j.java
7	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	fe/z.java ob/a.java ob/b.java pb/a.java r9/n.java te/d.java te/h.java x6/c.java
8	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	g9/b.java k2/c.java
9	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	com/reactnativecommunity/clipboard/ClipboardModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	m8/w.java
12	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/salesforce/marketingcloud/util/l.java
13	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	ea/b.java
14	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	q4/a.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	g9/c.java r4/a.java
00013	Read file and put it into a stream	file	com/airbnb/android/react/maps/f.java com/airbnb/android/react/maps/n.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnativecommunity/asyncstorage/c.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/rnfs/RNFSManager.java com/rnfs/i.java com/salesforce/marketingcloud/storage/f.java com/salesforce/marketingcloud/tozny/AesCbcWithIntegrity.java com/salesforce/marketingcloud/util/e.java com/salesforce/marketingcloud/util/f.java com/salesforce/marketingcloud/util/g.java g9/c.java k1/g.java k1/h.java r4/a.java s3/d.java ta/e.java ue/r.java v1/b.java
00026	Method reflection	reflection	gc/a.java gc/b.java
00114	Create a secure socket connection to the proxy address	network command	ke/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	b2/c.java com/oblador/vectoricons/a.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnative/ivpusic/imagepicker/a.java com/reactnative/ivpusic/imagepicker/e.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/rnfs/RNFSManager.java com/salesforce/marketingcloud/storage/f.java com/salesforce/marketingcloud/util/e.java fr/greweb/reactnativeviewshot/RNViewShotModule.java h2/a.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java k1/g.java k1/h.java x1/f.java z0/b.java z0/d.java z0/e.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/a.java com/salesforce/marketingcloud/storage/db/d.java com/salesforce/marketingcloud/storage/db/f.java com/salesforce/marketingcloud/storage/db/m.java com/salesforce/marketingcloud/storage/db/upgrades/i.java
00036	Get resource file from res/raw directory	reflection	com/airbnb/android/react/maps/g.java com/airbnb/android/react/maps/q.java com/reactnativecommunity/toolbarandroid/b.java com/salesforce/marketingcloud/notifications/b.java f5/a.java h6/f.java ma/d.java z0/b.java
00147	Get the time of current location	collection location	com/reactnativecommunity/geolocation/GeolocationModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00075	Get location of the device	collection location	com/reactnativecommunity/geolocation/GeolocationModule.java
00137	Get last known location of the device	location collection	com/reactnativecommunity/geolocation/GeolocationModule.java
00115	Get last known location of the device	collection location	com/reactnativecommunity/geolocation/GeolocationModule.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	a1/g.java a1/n.java cl/json/RNShareModule.java com/cslplasma/opensettings/OpenSettingsModule.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/salesforce/marketingcloud/notifications/b.java h6/f.java
00189	Get the content of a SMS message	sms	com/imagepicker/i.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/rt2zz/reactnativecontacts/a.java com/vonovak/a.java k2/f.java
00192	Get messages in the SMS inbox	sms	com/reactnativecommunity/cameraroll/CameraRollModule.java com/rnfs/RNFSManager.java z0/b.java
00188	Get the address of a SMS message	sms	com/imagepicker/i.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/rt2zz/reactnativecontacts/a.java com/vonovak/a.java k2/f.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/reactnativecommunity/cameraroll/CameraRollModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00121	Create a directory	file command	com/reactnativecommunity/cameraroll/CameraRollModule.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/reactnativecommunity/cameraroll/CameraRollModule.java
00125	Check if the given file path exist	file	com/reactnativecommunity/cameraroll/CameraRollModule.java
00191	Get messages in the SMS inbox	sms	com/reactnativecommunity/cameraroll/CameraRollModule.java
00200	Query data from the contact list	collection contact	com/imagepicker/i.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/rt2zz/reactnativecontacts/a.java com/vonovak/a.java k2/f.java
00187	Query a URI and check the result	collection sms calllog calendar	com/reactnativecommunity/cameraroll/CameraRollModule.java com/rt2zz/reactnativecontacts/a.java
00104	Check if the given path is directory	file	com/reactnativecommunity/cameraroll/CameraRollModule.java
00201	Query data from the call log	collection calllog	com/imagepicker/i.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/rt2zz/reactnativecontacts/a.java com/vonovak/a.java k2/f.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/imagepicker/i.java com/reactnativecommunity/cameraroll/CameraRollModule.java
00096	Connect to a URL and set request method	command network	com/salesforce/marketingcloud/http/b.java com/salesforce/marketingcloud/media/q.java h9/c.java k1/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	com/rnfs/c.java com/salesforce/marketingcloud/http/b.java com/salesforce/marketingcloud/media/q.java com/salesforce/marketingcloud/notifications/b.java h9/c.java
00162	Create InetSocketAddress object and connecting to it	socket	pe/b.java pe/j.java
00163	Create new Socket and connecting to it	socket	pe/b.java pe/j.java
00091	Retrieve data from broadcast	collection	com/salesforce/marketingcloud/alarms/b.java com/salesforce/marketingcloud/messages/push/a.java la/f.java
00024	Write file after Base64 decoding	reflection file	com/salesforce/marketingcloud/tozny/AesCbcWithIntegrity.java z0/d.java z0/e.java
00043	Calculate WiFi signal strength	collection wifi	aa/c.java
00109	Connect to a URL and get the response code	network command	com/rnfs/c.java com/salesforce/marketingcloud/http/b.java e6/f.java h9/c.java z5/d.java
00030	Connect to the remote server through the given URL	network	com/rnfs/c.java com/salesforce/marketingcloud/notifications/b.java k1/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00078	Get the network operator name	collection telephony	com/learnium/RNDeviceInfo/RNDeviceModule.java
00038	Query the phone number	collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00130	Get the current WIFI information	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00134	Get the current WiFi IP address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceModule.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	a1/g.java com/cslplasma/opensettings/OpenSettingsModule.java h6/f.java
00028	Read file from assets directory	file	com/rnfs/RNFSManager.java
00016	Get location info of the device and put it to JSON object	location collection	com/salesforce/marketingcloud/messages/d.java
00175	Get notification manager and cancel notifications	notification	na/c.java
00072	Write HTTP input stream into a file	command network file	com/rnfs/c.java
00012	Read data and put it into a buffer stream	file	com/rnfs/i.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://coral-shift-272205.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/745320931609/namespaces/firebase:fetch?key=AIzaSyCUmFjoUfwczIxsTtz83YVKMQVQXADf0_A. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/25	android.permission.RECEIVE_BOOT_COMPLETED, android.permission.VIBRATE, android.permission.INTERNET, android.permission.CAMERA, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_FINE_LOCATION, android.permission.READ_CONTACTS, android.permission.GET_ACCOUNTS, android.permission.WAKE_LOCK, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_COARSE_LOCATION
Other Common Permissions	5/44	android.permission.WRITE_CONTACTS, android.permission.READ_CALENDAR, com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
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
twitter.com	ok	**IP:** 172.66.0.227 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
stage.app.igodigital.com	ok	**IP:** 98.86.87.253 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
developer.android.com	ok	**IP:** 64.233.176.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
accounts.google.com	ok	**IP:** 172.217.215.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
mcp3nmv2h4xn0bwjnf35611cvwn1.device.marketingcloudapis.com	ok	**IP:** 13.110.204.30 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.788464 **Longitude:** -122.394608 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
coral-shift-272205.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
salesforce-marketingcloud.github.io	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
plus.google.com	ok	**IP:** 64.233.185.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app.igodigital.com	ok	**IP:** 3.223.223.172 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 64.233.177.155 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 172.253.124.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	h6/w.java

TRACKERS

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Salesforce Marketing Cloud		https://reports.exodus-privacy.eu.org/trackers/220

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://coral-shift-272205.firebaseio.com"
"google_api_key" : "AIzaSyCUmFjoUfwczIxsTtz83YVKMQVQXADf0_A"
"google_crash_reporting_api_key" : "AIzaSyCUmFjoUfwczIxsTtz83YVKMQVQXADf0_A"
e78b87e2-89c9-4525-995d-cb7d3be11050

POSSIBLE SECRETS
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
F6389234-1024-481F-9173-37D9D7F5051F
849f26e2-2df6-11e4-ab12-14109fdc48df
29200FA5-DF79-4C3F-BC0F-E2FF3CE6199A

PLAYSTORE INFORMATION

Title: CSL Plasma

Score: 4.0729847 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.cslplasma.cslplasmadonorapplication

Developer Details: CSL PLASMA INC., CSL+PLASMA+INC., None, https://www.cslplasma.com/contact-us, cslplasma.google@cslplasma.com,

Release Date: Jul 22, 2020 **Privacy Policy:** Privacy link

Description:

Save time and manage your rewards! Download the app and get more out of every donation. Complete your online health screening, skip the kiosk line and activate your iGive Rewards® to start earning additional points you can redeem for cash. Get the CSL Plasma App to: • Get updates and learn about local promotions • Manage reward points • Launch your Donor360® health questionnaire to start your visit before you arrive • Refer friends and earn reward points Make your donation process a better experience with the CSL Plasma App. Use the CSL Plasma App to find your center, see your first month rewards, get donation tips and connect with customer service. You will get your donor ID when you register at your local CSL Plasma Center. If you already have your donor ID, download the App and get started! Help save lives, while making a difference in your own. Do the AMAZING. Donate plasma today. For more information about CSL Plasma please go to www.cslplasma.com

SCAN LOGS

Timestamp	Event	Error

2025-08-29 21:23:49	Generating Hashes	OK
2025-08-29 21:23:49	Extracting APK	OK
2025-08-29 21:23:49	Unzipping	OK
2025-08-29 21:23:50	Parsing APK with androguard	OK
2025-08-29 21:23:50	Extracting APK features using aapt/aapt2	OK
2025-08-29 21:23:50	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 21:23:52	Parsing AndroidManifest.xml	OK
2025-08-29 21:23:52	Extracting Manifest Data	OK
2025-08-29 21:23:52	Manifest Analysis Started	OK
2025-08-29 21:23:52	Performing Static Analysis on: CSL Plasma (com.cslplasma.cslplasmadonorapplication)	OK
2025-08-29 21:23:53	Fetching Details from Play Store: com.cslplasma.cslplasmadonorapplication	OK

2025-08-29 21:23:53	Checking for Malware Permissions	OK
2025-08-29 21:23:53	Fetching icon path	OK
2025-08-29 21:23:53	Library Binary Analysis Started	OK
2025-08-29 21:23:53	Reading Code Signing Certificate	OK
2025-08-29 21:23:54	Running APKiD 2.1.5	OK
2025-08-29 21:23:56	Detecting Trackers	OK
2025-08-29 21:23:58	Decompiling APK to Java with JADX	OK
2025-08-29 21:24:13	Converting DEX to Smali	OK
2025-08-29 21:24:13	Code Analysis Started on - java_source	OK
2025-08-29 21:24:15	Android SBOM Analysis Completed	OK
2025-08-29 21:24:24	Android SAST Completed	OK

2025-08-29 21:24:24	Android API Analysis Started	OK
2025-08-29 21:24:34	Android API Analysis Completed	OK
2025-08-29 21:24:34	Android Permission Mapping Started	OK
2025-08-29 21:24:43	Android Permission Mapping Completed	OK
2025-08-29 21:24:43	Android Behaviour Analysis Started	OK
2025-08-29 21:25:05	Android Behaviour Analysis Completed	OK
2025-08-29 21:25:05	Extracting Emails and URLs from Source Code	OK
2025-08-29 21:25:08	Email and URL Extraction Completed	OK
2025-08-29 21:25:08	Extracting String data from APK	OK
2025-08-29 21:25:08	Extracting String data from Code	OK
2025-08-29 21:25:08	Extracting String values and entropies from Code	OK

2025-08-29 21:25:10	Performing Malware check on extracted domains	OK
2025-08-29 21:25:15	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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.