MOBSF

ANDROID STATIC ANALYSIS REPORT

YouTube (16.25.39)

File Name: YouTube.apk

Package Name:	com.google.android.youtube
Scan Date:	March 19, 2024, 6:21 a.m.
App Security Score:	47/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
6	59	2	2	1

FILE INFORMATION

File Name: YouTube.apk
Size: 93.41MB
MD5: ed3904ea2e7edba134bb33877779aba1
SHA1: 00dc7cb2d1436f58d59644eb177b8d1d73fd9098
SHA256: 880364e2d82167c9ec11904d8d289acb2c8d831cf4f3e5ae940b9f3443a7e6a6

APP INFORMATION

App Name: YouTube
Package Name: com.google.android.youtube
Main Activity: com.google.android.apps.youtube.app.application.Shell_SettingsActivity
Target SDK: 30
Min SDK: 21
Max SDK:
Android Version Name: 16.25.39
Android Version Code: 1521745368

APP COMPONENTS

Activities: 52
Services: 22

Receivers: 32
Providers: 3
Exported Activities: 26
Exported Services: 4
Exported Receivers: 15
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=CA, L=Mountain View, O=Google, Inc, OU=Google, Inc, CN=Unknown
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2008-12-02 02:07:58+00:00
Valid To: 2036-04-19 02:07:58+00:00
Issuer: C=US, ST=CA, L=Mountain View, O=Google, Inc, OU=Google, Inc, CN=Unknown
Serial Number: 0x4934987e
Hash Algorithm: md5
md5: d046fc5d1fc3cd0e57c5444097cd5449
sha1: 24bb24c05e47e0aefa68a58a766179d9b613a600
sha256: 3d7a1223019aa39d9ea0e3436ab7c0896bfb4fb679f4de5fe7c23f326c8f994a
sha512: 696a69f617980d711da35cce1fe6bddf2f3b76714d51758c5d1cef8f28eb3033371561c693c0819a57d07391a8cde08c99c92688c962252ffab21297e2df8e8e
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 516ad3a6ae407da983ae7fd992217217ef8b7959a0d1711546a7dcc67f8e7460
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.MANAGE_DOCUMENTS	signature	allows management of document access, typically in a picker.	Allows an application to manage access to documents, usually as part of a document picker.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.

PERMISSION	STATUS	INFO	DESCRIPTION
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
com.google.android.gms.permission.AD_ID_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.youtube.permission.C2D_MESSAGE	signature	Allows cloud to device messaging	Allows the application to receive push notifications.
android.permission.GET_PACKAGE_SIZE	normal	measure application storage space	Allows an application to find out the space used by any package.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
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.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.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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
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.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.
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.
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.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>/home/mobsf/.MobSF/uploads/ed3904ea2e7edba134bb33877779aba1/ed3904ea2e7edba134bb33877779aba1.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Obfuscator</td><td>DexGuard</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></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
Build.HARDWARE check
Build.TAGS check
SIM operator check
network operator name check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.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
Build.HARDWARE check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.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
Build.HARDWARE check
Build.BOARD check
Build.TAGS check
SIM operator check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
<tr><td>classes4.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.HARDWARE check
possible Build.SERIAL check
Build.TAGS check
SIM operator check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes5.dex	FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
net.openid.appauth.RedirectUriReceiverActivity	Schemes: vnd.youtube.gdi://,
com.google.android.youtube.UrlActivity	Schemes: http://, https://, vnd.youtube://, vnd.youtube.launch://, Hosts: youtube.com, www.youtube.com, m.youtube.com, youtu.be, Path Patterns: .*,
com.google.android.apps.youtube.app.extensions.accountlinking.UriFlowActivity	Schemes: vnd.youtube.uriflow://,
com.google.android.libraries.accountlinking.activity.AccountLinkingActivity	Schemes: com.google.android.apps.youtube://, Hosts: oauth2redirect,

NETWORK SECURITY

HIGH: 1 | WARNING: 1 | INFO: 0 | SECURE: 1

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.

NO	SCOPE	SEVERITY	DESCRIPTION
3	youtube.com googleapis.com	secure	Domain config is securely configured to disallow clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 1 | 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 vulnerable to hash collision	high	Application is signed with MD5. MD5 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 46 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag 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.
4	Broadcast Receiver (com.google.android.libraries.youtube.player.ui.mediasession.MediaButtonIntentReceiverProvider$DefaultMediaButtonIntentReceiver) 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	Activity (net.openid.appauth.RedirectUriReceiverActivity) is not Protected. [android:exported=true]	warning	An Activity 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	Activity (com.google.android.youtube.api.StandalonePlayerActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INTERNET [android:exported=true]	warning	An Activity 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.youtube.api.service.YouTubeService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INTERNET [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.

NO	ISSUE	SEVERITY	DESCRIPTION
8	Activity (com.google.android.apps.youtube.app.application.Shell_HomeActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Activity-Alias (com.google.android.youtube.HomeActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Activity-Alias (com.google.android.youtube.app.application.Shell$HomeActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Activity-Alias (com.google.android.youtube.app.honeycomb.Shell$HomeActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias 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
12	Activity (com.google.android.apps.youtube.app.application.Shell_UrlActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Activity-Alias (com.google.android.apps.youtube.app.application.Shell$UrlActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
14	Activity-Alias (com.google.android.youtube.UrlActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
15	Activity (com.google.android.apps.youtube.app.application.Shell_ResultsActivity) is not Protected. [android:exported=true]	warning	An Activity 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
16	Activity-Alias (com.google.android.apps.youtube.app.application.Shell$ResultsActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
17	Activity (com.google.android.apps.youtube.app.application.Shell_MediaSearchActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
18	Activity-Alias (com.google.android.apps.youtube.app.application.Shell$MediaSearchActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
19	Activity (com.google.android.apps.youtube.app.application.Shell_UploadActivity) is not Protected. [android:exported=true]	warning	An Activity 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
20	Activity-Alias (com.google.android.youtube.UploadIntentHandlingActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
21	Activity-Alias (com.google.android.apps.youtube.app.application.Shell$UploadActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
22	Activity (com.google.android.apps.youtube.app.application.Shell_LiveCreationActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
23	Activity-Alias (com.google.android.apps.youtube.app.application.Shell$LiveCreationActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias 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
24	Activity-Alias (com.google.android.apps.youtube.app.application.Shell$SettingsActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
25	Activity-Alias (com.google.android.youtube.ManageNetworkUsageActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
26	Broadcast Receiver (com.google.android.apps.youtube.app.application.backup.PackageReplacedReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
27	Broadcast Receiver (com.google.android.apps.youtube.app.application.system.LocaleUpdatedReceiver) 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.
28	Service (com.google.android.apps.youtube.app.common.notification.FcmMessageListenerService) 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.
29	Activity (com.google.android.apps.youtube.app.extensions.accountlinking.UriFlowActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
30	Activity (com.google.android.libraries.accountlinking.activity.AccountLinkingActivity) is not Protected. [android:exported=true]	warning	An Activity 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
31	Service (com.google.android.apps.youtube.app.extensions.mediabrowser.impl.MainAppMediaBrowserService) 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.
32	Activity (com.google.android.apps.youtube.app.watchwhile.WatchWhileActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
33	Activity-Alias (com.google.android.apps.youtube.app.WatchWhileActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
34	Broadcast Receiver (com.google.android.libraries.notifications.entrypoints.accountchanged.AccountChangedReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
35	Broadcast Receiver (com.google.android.libraries.notifications.entrypoints.blockstatechanged.BlockStateChangedReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
36	Broadcast Receiver (com.google.android.libraries.notifications.entrypoints.gcm.GcmBroadcastReceiver) 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
37	Broadcast Receiver (com.google.android.libraries.notifications.entrypoints.localechanged.LocaleChangedReceiver) 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.
38	Broadcast Receiver (com.google.android.libraries.notifications.entrypoints.phenotype.PhenotypeUpdateReceiver) 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.
39	Broadcast Receiver (com.google.android.libraries.notifications.entrypoints.restart.RestartReceiver) 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.
40	Broadcast Receiver (com.google.android.libraries.notifications.entrypoints.timezonechanged.TimezoneChangedReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
41	Broadcast Receiver (com.google.android.libraries.phenotype.client.stable.AccountRemovedBroadcastReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
42	Broadcast Receiver (com.google.android.libraries.phenotype.client.stable.PhenotypeUpdateBackgroundBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.PHENOTYPE_UPDATE_BROADCAST [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
43	Activity (com.google.android.libraries.social.licenses.LicenseMenuActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
44	Broadcast Receiver (com.google.android.libraries.youtube.account.service.AccountsChangedReceiver) 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.
45	Activity (com.google.cardboard.sdk.HeadsetDetectionActivity) is not Protected. [android:exported=true]	warning	An Activity 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
46	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
47	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.

NO	ISSUE	SEVERITY	DESCRIPTION
48	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.

</> CODE ANALYSIS

HIGH: 3 | WARNING: 9 | INFO: 2 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/a.java defpackage/aan.java defpackage/aap.java defpackage/aaqh.java defpackage/aarc.java defpackage/aaui.java defpackage/aayg.java defpackage/aazf.java defpackage/aazw.java defpackage/abbz.java defpackage/abcs.java defpackage/abf.java defpackage/abfe.java defpackage/abfg.java defpackage/abfj.java defpackage/abfo.java defpackage/abfq.java defpackage/abfy.java defpackage/abga.java defpackage/abgd.java defpackage/abgi.java defpackage/abgk.java defpackage/abgn.java defpackage/abgo.java defpackage/abgp.java defpackage/abgq.java defpackage/abgw.java defpackage/abha.java defpackage/abhb.java defpackage/abhc.java defpackage/abhd.java defpackage/abhi.java defpackage/abhk.java defpackage/abho.java defpackage/abhr.java defpackage/abip.java defpackage/abiq.java defpackage/abis.java defpackage/abiu.java defpackage/abiy.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/abju.java defpackage/abjx.java defpackage/abka.java defpackage/abkf.java defpackage/abkg.java defpackage/abpu.java defpackage/acgv.java defpackage/acs.java defpackage/adcj.java defpackage/adn.java defpackage/adr.java defpackage/adu.java defpackage/aea.java defpackage/aeb.java defpackage/aee.java defpackage/aes.java defpackage/aeu.java defpackage/aeuh.java defpackage/aew.java defpackage/aey.java defpackage/afy.java defpackage/agda.java defpackage/agm.java defpackage/agsi.java defpackage/ahgs.java defpackage/ahm.java defpackage/aidk.java defpackage/aisi.java defpackage/aisk.java defpackage/aiw.java defpackage/ajg.java defpackage/ajmh.java defpackage/akdu.java defpackage/akf.java defpackage/akgu.java defpackage/akh.java defpackage/akil.java defpackage/akiu.java defpackage/akjr.java defpackage/akkb.java defpackage/aknu.java defpackage/akqh.java defpackage/akrd.java defpackage/akro.java defpackage/aksc.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/aksd.java defpackage/aksk.java defpackage/aksq.java defpackage/aksv.java defpackage/aksy.java defpackage/akte.java defpackage/aktf.java defpackage/aktw.java defpackage/akw.java defpackage/albz.java defpackage/alci.java defpackage/aluo.java defpackage/aluz.java defpackage/alvd.java defpackage/amog.java defpackage/ampf.java defpackage/ampp.java defpackage/ampw.java defpackage/amrw.java defpackage/amrz.java defpackage/amsb.java defpackage/amse.java defpackage/amsh.java defpackage/amsw.java defpackage/amta.java defpackage/amti.java defpackage/amtn.java defpackage/amtq.java defpackage/amtr.java defpackage/amua.java defpackage/amuc.java defpackage/amue.java defpackage/amuf.java defpackage/amuj.java defpackage/amum.java defpackage/amup.java defpackage/amuq.java defpackage/amur.java defpackage/amuv.java defpackage/amvc.java defpackage/amyl.java defpackage/amyo.java defpackage/amzh.java defpackage/amzi.java defpackage/amzs.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/anaw.java defpackage/aph.java defpackage/apk.java defpackage/apo.java defpackage/aqo.java defpackage/aqy.java defpackage/ard.java defpackage/arw.java defpackage/arx.java defpackage/ary.java defpackage/asa.java defpackage/asb.java defpackage/ase.java defpackage/asn.java defpackage/at.java defpackage/atp.java defpackage/atv.java defpackage/aua.java defpackage/aug.java defpackage/auo.java defpackage/aup.java defpackage/aus.java defpackage/aut.java defpackage/av.java defpackage/avow.java defpackage/avoy.java defpackage/avoz.java defpackage/avpa.java defpackage/avpb.java defpackage/avpe.java defpackage/avpf.java defpackage/avpg.java defpackage/avpr.java defpackage/avpv.java defpackage/avpx.java defpackage/avqn.java defpackage/avr.java defpackage/avrb.java defpackage/avrf.java defpackage/avwi.java defpackage/awhw.java defpackage/awj.java defpackage/awl.java defpackage/awmx.java defpackage/awp.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/ax.java defpackage/axh.java defpackage/ayhp.java defpackage/ayih.java defpackage/aylc.java defpackage/aylm.java defpackage/ayln.java defpackage/aylr.java defpackage/aymc.java defpackage/ayn.java defpackage/ayvh.java defpackage/azd.java defpackage/azn.java defpackage/azw.java defpackage/azx.java defpackage/bcu.java defpackage/bdf.java defpackage/beb.java defpackage/bej.java defpackage/brd.java defpackage/bsr.java defpackage/bun.java defpackage/byu.java defpackage/bzj.java defpackage/bzt.java defpackage/cbk.java defpackage/ccx.java defpackage/cda.java defpackage/cej.java defpackage/ces.java defpackage/cfe.java defpackage/cfs.java defpackage/cfv.java defpackage/cfz.java defpackage/cha.java defpackage/cia.java defpackage/clj.java defpackage/cls.java defpackage/cmi.java defpackage/cmk.java defpackage/cnn.java defpackage/cqa.java defpackage/cri.java defpackage/csd.java defpackage/cv.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/dbg.java defpackage/dca.java defpackage/dcb.java defpackage/dcf.java defpackage/dch.java defpackage/dci.java defpackage/dcl.java defpackage/dcn.java defpackage/dcr.java defpackage/dda.java defpackage/dgz.java defpackage/dil.java defpackage/dir.java defpackage/dka.java defpackage/dlh.java defpackage/dp.java defpackage/dr.java defpackage/dvb.java defpackage/eax.java defpackage/etf.java defpackage/fk.java defpackage/fqi.java defpackage/ft.java defpackage/fz.java defpackage/gdr.java defpackage/guh.java defpackage/gv.java defpackage/hj.java defpackage/hm.java defpackage/hn.java defpackage/htr.java defpackage/ib.java defpackage/ig.java defpackage/ih.java defpackage/ii.java defpackage/ij.java defpackage/ik.java defpackage/ip.java defpackage/iu.java defpackage/jh.java defpackage/jt.java defpackage/jv.java defpackage/jx.java defpackage/ka.java defpackage/kaj.java
	The App logs information. Sensitive		CWE: CWE-532: Insertion of Sensitive Information into Log File	

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	defpackage/kaj.java defpackage/kez.java defpackage/kf.java defpackage/kg.java defpackage/kn.java defpackage/ku.java defpackage/kuo.java defpackage/kv.java defpackage/ly.java defpackage/mf.java defpackage/mk.java defpackage/nqg.java defpackage/nxh.java defpackage/nyd.java defpackage/nyx.java defpackage/nzy.java defpackage/oaw.java defpackage/obg.java defpackage/odz.java defpackage/oec.java defpackage/oeu.java defpackage/oez.java defpackage/ofh.java defpackage/ofi.java defpackage/ofq.java defpackage/ofu.java defpackage/ogq.java defpackage/ogx.java defpackage/ohs.java defpackage/oil.java defpackage/oit.java defpackage/oiu.java defpackage/ojg.java defpackage/ojo.java defpackage/ojt.java defpackage/oju.java defpackage/ojw.java defpackage/okh.java defpackage/okm.java defpackage/ols.java defpackage/oma.java defpackage/omh.java defpackage/onc.java defpackage/ong.java defpackage/onm.java defpackage/oqu.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/oqd.java defpackage/ora.java defpackage/osn.java defpackage/ovm.java defpackage/owt.java defpackage/owx.java defpackage/owz.java defpackage/oxe.java defpackage/oxo.java defpackage/oxq.java defpackage/oxv.java defpackage/oxw.java defpackage/oyc.java defpackage/oys.java defpackage/oyz.java defpackage/ozi.java defpackage/ozm.java defpackage/ozn.java defpackage/ozs.java defpackage/paj.java defpackage/pao.java defpackage/pbi.java defpackage/pbk.java defpackage/pbw.java defpackage/pcn.java defpackage/pem.java defpackage/pfb.java defpackage/pfn.java defpackage/pft.java defpackage/pgz.java defpackage/ph.java defpackage/phd.java defpackage/phi.java defpackage/phv.java defpackage/phz.java defpackage/pib.java defpackage/pid.java defpackage/pii.java defpackage/pin.java defpackage/piw.java defpackage/pix.java defpackage/pku.java defpackage/plk.java defpackage/pmv.java defpackage/pnj.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/pod.java defpackage/poe.java defpackage/poi.java defpackage/pop.java defpackage/pot.java defpackage/pwp.java defpackage/pzc.java defpackage/pzg.java defpackage/pzi.java defpackage/qc.java defpackage/qff.java defpackage/qgx.java defpackage/qhn.java defpackage/qhy.java defpackage/qid.java defpackage/qie.java defpackage/qik.java defpackage/qip.java defpackage/qiq.java defpackage/qiu.java defpackage/qiv.java defpackage/qjf.java defpackage/qjk.java defpackage/qjl.java defpackage/qkq.java defpackage/qkr.java defpackage/qlf.java defpackage/qlt.java defpackage/qlv.java defpackage/qlx.java defpackage/qmx.java defpackage/qmy.java defpackage/qnn.java defpackage/qns.java defpackage/qnx.java defpackage/qnz.java defpackage/qod.java defpackage/qog.java defpackage/qom.java defpackage/qon.java defpackage/qov.java defpackage/qox.java defpackage/qpp.java defpackage/qpq.java defpackage/qpu.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/qqb.java defpackage/qqv.java defpackage/qrl.java defpackage/qrp.java defpackage/qrx.java defpackage/qsi.java defpackage/qsu.java defpackage/qsv.java defpackage/qtb.java defpackage/qtc.java defpackage/qtd.java defpackage/qux.java defpackage/quy.java defpackage/qvb.java defpackage/qvd.java defpackage/qve.java defpackage/qwb.java defpackage/qwg.java defpackage/qxp.java defpackage/qyd.java defpackage/qyo.java defpackage/qzm.java defpackage/rbo.java defpackage/ris.java defpackage/rj.java defpackage/rji.java defpackage/rjt.java defpackage/rkd.java defpackage/rko.java defpackage/rl.java defpackage/rla.java defpackage/rmp.java defpackage/rmq.java defpackage/rna.java defpackage/rnd.java defpackage/rnz.java defpackage/roe.java defpackage/roh.java defpackage/rru.java defpackage/rui.java defpackage/ruo.java defpackage/rvv.java defpackage/ryx.java defpackage/rze.java defpackage/sb.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/sc.java defpackage/sck.java defpackage/siu.java defpackage/sjb.java defpackage/sjf.java defpackage/spu.java defpackage/sqa.java defpackage/sqb.java defpackage/sqe.java defpackage/sqm.java defpackage/ssb.java defpackage/stf.java defpackage/suk.java defpackage/sz.java defpackage/tej.java defpackage/tfh.java defpackage/tfy.java defpackage/tic.java defpackage/tif.java defpackage/tlh.java defpackage/tli.java defpackage/tlz.java defpackage/toa.java defpackage/toq.java defpackage/tpy.java defpackage/trm.java defpackage/tsl.java defpackage/tul.java defpackage/tww.java defpackage/txf.java defpackage/txi.java defpackage/txv.java defpackage/tyh.java defpackage/tyt.java defpackage/tzh.java defpackage/tzi.java defpackage/ubc.java defpackage/uhl.java defpackage/uhs.java defpackage/uhu.java defpackage/uhv.java defpackage/uhz.java defpackage/uia.java defpackage/uib.java defpackage/uid.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/uiy.java defpackage/ujc.java defpackage/ujo.java defpackage/ujx.java defpackage/uka.java defpackage/uke.java defpackage/ukk.java defpackage/ukm.java defpackage/ukn.java defpackage/ukp.java defpackage/ulg.java defpackage/umu.java defpackage/upn.java defpackage/upq.java defpackage/upv.java defpackage/uqc.java defpackage/uwh.java defpackage/uyd.java defpackage/uyp.java defpackage/vc.java defpackage/vej.java defpackage/vg.java defpackage/vkk.java defpackage/vt.java defpackage/wi.java defpackage/wj.java defpackage/xki.java defpackage/xmz.java defpackage/xn.java defpackage/xtb.java defpackage/yfp.java defpackage/ykg.java defpackage/yn.java defpackage/yod.java defpackage/ytz.java defpackage/yz.java defpackage/zb.java defpackage/zf.java defpackage/zi.java defpackage/zj.java defpackage/zm.java
				defpackage/abgw.java defpackage/abxi.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	defpackage/abyy.java defpackage/ace.java defpackage/acs.java defpackage/acvl.java defpackage/adkb.java defpackage/adra.java defpackage/adyd.java defpackage/aebs.java defpackage/aeld.java defpackage/ahsi.java defpackage/aifr.java defpackage/ajed.java defpackage/akwv.java defpackage/aley.java defpackage/amol.java defpackage/avjy.java defpackage/avkc.java defpackage/awqc.java defpackage/awqf.java defpackage/awqh.java defpackage/awug.java defpackage/ayam.java defpackage/aydv.java defpackage/dgh.java defpackage/dgz.java defpackage/dli.java defpackage/dlj.java defpackage/ers.java defpackage/exj.java defpackage/gag.java defpackage/oiu.java defpackage/ojg.java defpackage/onc.java defpackage/onm.java defpackage/pff.java defpackage/prt.java defpackage/qgp.java defpackage/qqw.java defpackage/rgn.java defpackage/rom.java defpackage/rri.java defpackage/tet.java defpackage/tfh.java defpackage/ugj.java defpackage/ugl.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/ugm.java defpackage/ugu.java defpackage/ugv.java defpackage/wcv.java defpackage/wfs.java defpackage/wfu.java defpackage/yju.java defpackage/zrj.java j$/util/concurrent/ThreadLocalRandom.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	defpackage/aetu.java defpackage/afgg.java defpackage/afii.java defpackage/afkl.java defpackage/afkv.java defpackage/afkx.java defpackage/afky.java defpackage/afkz.java defpackage/afla.java defpackage/afln.java defpackage/afwc.java defpackage/ajde.java defpackage/ajvo.java defpackage/amzo.java defpackage/azv.java defpackage/dca.java defpackage/dck.java defpackage/rad.java defpackage/rah.java defpackage/rap.java defpackage/rbi.java defpackage/rgc.java defpackage/rgi.java defpackage/rgr.java defpackage/tjj.java defpackage/tjl.java defpackage/tjn.java defpackage/tjp.java defpackage/tqe.java defpackage/uvo.java defpackage/uwd.java defpackage/vhb.java defpackage/xsg.java defpackage/xsj.java
4	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	defpackage/acyb.java defpackage/kjs.java defpackage/mke.java defpackage/rtg.java defpackage/wpz.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	defpackage/afok.java defpackage/afrt.java defpackage/afxe.java defpackage/aicf.java defpackage/ajso.java defpackage/ajve.java defpackage/ajxp.java defpackage/avpe.java defpackage/ayvh.java defpackage/gdg.java defpackage/guj.java defpackage/gzu.java defpackage/hl.java defpackage/hte.java defpackage/uqg.java defpackage/uqi.java defpackage/ylv.java defpackage/ytb.java defpackage/ytc.java
6	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	defpackage/ahmm.java defpackage/amru.java defpackage/amsw.java defpackage/amua.java defpackage/avpv.java defpackage/awbd.java defpackage/teu.java defpackage/vht.java
7	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	defpackage/adan.java defpackage/ajso.java defpackage/amsx.java defpackage/awam.java defpackage/dr.java defpackage/rsb.java defpackage/via.java defpackage/wvt.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	defpackage/akrf.java defpackage/dlj.java defpackage/uhu.java
9	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	defpackage/acen.java defpackage/acfc.java defpackage/aigf.java defpackage/awao.java defpackage/ymw.java
10	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	defpackage/iqt.java defpackage/tfy.java defpackage/vha.java
11	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	defpackage/ammw.java defpackage/anjz.java defpackage/awe.java defpackage/dcn.java defpackage/pxe.java defpackage/rgn.java defpackage/ssb.java defpackage/uwr.java
12	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	defpackage/ablf.java defpackage/agyg.java defpackage/ajgz.java defpackage/ayd.java defpackage/ebj.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	defpackage/adn.java defpackage/dgq.java defpackage/vkg.java
14	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	defpackage/tzi.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
15	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	defpackage/uik.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libfilterframework_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/libopusJNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
3	arm64-v8a/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__FD_CLR_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	arm64-v8a/libgvr_audio.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.
5	arm64-v8a/libelements.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	arm64-v8a/libgvr.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk', '__read_chk']	False warning Symbols are available.
7	arm64-v8a/libjsc.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	arm64-v8a/libgav1JNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.
9	arm64-v8a/libframesequence.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	arm64-v8a/libvpx.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
11	arm64-v8a/libcardboard_sdk_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	arm64-v8a/libdrishti_jni_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.
13	arm64-v8a/libnativecrashdetector.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	arm64-v8a/libtensorflowlite_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__strlen_chk']	False warning Symbols are available.
15	arm64-v8a/libvpxV2JNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	arm64-v8a/libyoga.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.
17	arm64-v8a/libvpxYTJNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	arm64-v8a/libopusV2JNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
19	arm64-v8a/libcardboard_api_only_gles2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	arm64-v8a/libcronet.93.0.4542.0.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__read_chk', '__vsnprintf_chk', '__memcpy_chk', '__FD_SET_chk', '__FD_CLR_chk', '__FD_ISSET_chk']	False warning Symbols are available.
21	arm64-v8a/libfilterframework_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	arm64-v8a/libopusJNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
23	arm64-v8a/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__FD_CLR_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	arm64-v8a/libgvr_audio.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.
25	arm64-v8a/libelements.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	arm64-v8a/libgvr.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk', '__read_chk']	False warning Symbols are available.
27	arm64-v8a/libjsc.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	arm64-v8a/libgav1JNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.
29	arm64-v8a/libframesequence.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
30	arm64-v8a/libvpx.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
31	arm64-v8a/libcardboard_sdk_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
32	arm64-v8a/libdrishti_jni_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.
33	arm64-v8a/libnativecrashdetector.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
34	arm64-v8a/libtensorflowlite_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__strlen_chk']	False warning Symbols are available.
35	arm64-v8a/libvpxV2JNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
36	arm64-v8a/libyoga.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.
37	arm64-v8a/libvpxYTJNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
38	arm64-v8a/libopusV2JNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
39	arm64-v8a/libcardboard_api_only_gles2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
40	arm64-v8a/libcronet.93.0.4542.0.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__read_chk', '__vsnprintf_chk', '__memcpy_chk', '__FD_SET_chk', '__FD_CLR_chk', '__FD_ISSET_chk']	False warning Symbols are available.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	15/24	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.GET_ACCOUNTS, android.permission.WAKE_LOCK, android.permission.CAMERA, android.permission.VIBRATE, android.permission.READ_CONTACTS, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.RECORD_AUDIO, android.permission.READ_PHONE_STATE, android.permission.SYSTEM_ALERT_WINDOW
Other Common Permissions	2/45	com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_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

DOMAIN	STATUS	GEOLOCATION
developers.cloudflare.com	ok	**IP:** 104.16.5.189 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase.google.com	ok	**IP:** 172.217.194.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
uytfe.sandbox.google.com	ok	**IP:** 74.125.130.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
alekberg.net	ok	No Geolocation information available.
xml.org	ok	**IP:** 104.239.240.11 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
google.com	ok	**IP:** 172.217.194.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
notifications-pa.googleapis.com	ok	**IP:** 74.125.68.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
plus.google.com	ok	**IP:** 172.217.194.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
imasdk.googleapis.com	ok	**IP:** 172.217.194.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
lh3.googleusercontent.com	ok	**IP:** 74.125.200.132 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developer.android.com	ok	**IP:** 172.253.118.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
dns11.quad9.net	ok	**IP:** 149.112.112.11 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.796986 **Longitude:** -122.462738 **View:** Google Map
lh4.googleusercontent.com	ok	**IP:** 74.125.200.132 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.googleapis.com	ok	**IP:** 142.251.10.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
doh.xfinity.com	ok	**IP:** 75.75.77.99 **Country:** United States of America **Region:** New Jersey **City:** Mount Laurel **Latitude:** 39.947819 **Longitude:** -74.911682 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
github.com	ok	**IP:** 20.205.243.166 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
dns.switch.ch	ok	**IP:** 130.59.31.251 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.ietf.org	ok	**IP:** 104.16.44.99 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.quad9.net	ok	**IP:** 216.21.3.77 **Country:** United States of America **Region:** California **City:** Berkeley **Latitude:** 37.879318 **Longitude:** -122.265205 **View:** Google Map
youtubei.googleapis.com	ok	**IP:** 142.251.10.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.nic.cz	ok	**IP:** 217.31.205.50 **Country:** Czechia **Region:** Praha, Hlavni mesto **City:** Prague **Latitude:** 50.088039 **Longitude:** 14.420760 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
symbolize.corp.google.com	ok	**IP:** 74.125.24.129 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
www.com	ok	**IP:** 45.33.20.235 **Country:** United States of America **Region:** Texas **City:** Richardson **Latitude:** 32.948181 **Longitude:** -96.729721 **View:** Google Map
exoplayer.dev	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.cisco.com	ok	**IP:** 23.49.9.16 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gl	ok	**IP:** 142.251.10.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
release-youtubei.sandbox.googleapis.com	ok	**IP:** 74.125.200.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
support.google.com	ok	**IP:** 74.125.130.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goto.google.com	ok	**IP:** 172.253.118.129 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 74.125.200.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
127.0.0.1	ok	**IP:** 127.0.0.1 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
www.oculus.com	ok	**IP:** 157.240.15.54 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
fonts.gstatic.com	ok	**IP:** 142.251.10.94 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
csi.gstatic.com	ok	**IP:** 216.239.32.3 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
myaccount.google.com	ok	**IP:** 74.125.68.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
doh.quickline.ch	ok	**IP:** 212.60.61.246 **Country:** Switzerland **Region:** Bern **City:** Biel **Latitude:** 47.132401 **Longitude:** 7.244110 **View:** Google Map
storage.googleapis.com	ok	**IP:** 172.253.118.207 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dnsnl.alekberg.net	ok	**IP:** 89.38.131.38 **Country:** Romania **Region:** Arges **City:** Curtea de Arges **Latitude:** 45.133331 **Longitude:** 24.683331 **View:** Google Map
www.google.com	ok	**IP:** 74.125.200.147 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
lh6.googleusercontent.com	ok	**IP:** 74.125.200.132 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
dns64.dns.google	ok	No Geolocation information available.
autopush-proddata-notifications-pa.sandbox.googleapis.com	ok	**IP:** 142.251.175.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
lh5.googleusercontent.com	ok	**IP:** 74.125.200.132 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.googleadservices.com	ok	**IP:** 74.125.200.154 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
suggestqueries.google.com	ok	**IP:** 74.125.24.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
dns.quad9.net	ok	**IP:** 9.9.9.9 **Country:** United States of America **Region:** California **City:** Berkeley **Latitude:** 37.879318 **Longitude:** -122.265205 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
app-measurement.com	ok	**IP:** 142.251.10.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
doh.dns.sb	ok	**IP:** 165.22.61.129 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
bit.ly	ok	**IP:** 67.199.248.10 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 64.233.170.156 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cami-youtubei.sandbox.googleapis.com	ok	**IP:** 64.233.170.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
com--android.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
autopush-notifications-pa.sandbox.googleapis.com	ok	**IP:** 74.125.24.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
upload.youtube.com	ok	**IP:** 172.217.194.117 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
chrome.cloudflare-dns.com	ok	**IP:** 162.159.61.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
dev-notifications-pa.corp.googleapis.com	ok	**IP:** 74.125.130.129 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
crbug.com	ok	**IP:** 216.239.32.29 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.webrtc.org	ok	**IP:** 172.253.118.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
nextdns.io	ok	**IP:** 104.26.10.186 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
doh.cleanbrowsing.org	ok	**IP:** 185.228.168.10 **Country:** United States of America **Region:** California **City:** Temecula **Latitude:** 33.530987 **Longitude:** -117.103394 **View:** Google Map
myactivity.google.com	ok	**IP:** 74.125.200.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dns.sb	ok	**IP:** 185.222.222.222 **Country:** Belgium **Region:** Brussels Hoofdstedelijk Gewest **City:** Brussels **Latitude:** 50.850449 **Longitude:** 4.348780 **View:** Google Map
doh-02.spectrum.com	ok	**IP:** 24.240.146.8 **Country:** United States of America **Region:** Louisiana **City:** Monroe **Latitude:** 32.509312 **Longitude:** -92.119301 **View:** Google Map
green-youtubei.sandbox.googleapis.com	ok	**IP:** 74.125.130.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
families.youtube.com	ok	**IP:** 74.125.200.190 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
odvr.nic.cz	ok	**IP:** 185.43.135.1 **Country:** Czechia **Region:** Praha, Hlavni mesto **City:** Prague **Latitude:** 50.088039 **Longitude:** 14.420760 **View:** Google Map
public.dns.iij.jp	ok	**IP:** 103.2.57.5 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
m.youtube.com	ok	**IP:** 74.125.130.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
youtube.com	ok	**IP:** 172.253.118.91 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dns10.quad9.net	ok	**IP:** 149.112.112.10 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.796986 **Longitude:** -122.462738 **View:** Google Map
www.example.com	ok	**IP:** 93.184.216.34 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
dummy.googlevideo.com	ok	No Geolocation information available.
doh.opendns.com	ok	**IP:** 146.112.41.2 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
staging-notifications-pa.sandbox.googleapis.com	ok	**IP:** 64.233.170.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
admob-gmats.uc.r.appspot.com	ok	**IP:** 142.251.175.153 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developers.google.com	ok	**IP:** 142.251.175.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
doh.familyshield.opendns.com	ok	**IP:** 146.112.41.3 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
doh-01.spectrum.com	ok	**IP:** 24.240.146.7 **Country:** United States of America **Region:** Louisiana **City:** Monroe **Latitude:** 32.509312 **Longitude:** -92.119301 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
googleads.g.doubleclick.net	ok	**IP:** 142.251.175.156 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
chromium.dns.nextdns.io	ok	**IP:** 194.156.163.172 **Country:** Belgium **Region:** Brussels Hoofdstedelijk Gewest **City:** Brussels **Latitude:** 50.850449 **Longitude:** 4.348780 **View:** Google Map
dns.google	ok	**IP:** 8.8.8.8 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
test-youtubei.sandbox.googleapis.com	ok	**IP:** 142.251.12.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.youtube.com	ok	**IP:** 74.125.200.190 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
cleanbrowsing.org	ok	**IP:** 45.77.168.207 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
accounts.google.com	ok	**IP:** 74.125.200.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
aomediacodec.github.io	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.gstatic.com	ok	**IP:** 74.125.130.94 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

FIREBASE DATABASES

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

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	defpackage/dcr.java
u0013android@android.com0 u0013android@android.com	defpackage/qjb.java
appro@openssl.org android-prod-builder@oqbn20.prod	lib/arm64-v8a/libjingle_peerconnection_so.so
android-prod-builder@oqbn20.prod	lib/arm64-v8a/libgvr_audio.so

EMAIL	FILE
android-prod-builder@oqbn20.prod	lib/arm64-v8a/libelements.so
android-prod-builder@oqbn20.prod	lib/arm64-v8a/libgvr.so
android-prod-builder@oqbn20.prod	lib/arm64-v8a/libgav1JNI.so
android-prod-builder@oqbn20.prod	lib/arm64-v8a/libdrishti_jni_native.so
appro@openssl.org	lib/arm64-v8a/libcronet.93.0.4542.0.so
appro@openssl.org android-prod-builder@oqbn20.prod	apktool_out/lib/arm64-v8a/libjingle_peerconnection_so.so
android-prod-builder@oqbn20.prod	apktool_out/lib/arm64-v8a/libgvr_audio.so
android-prod-builder@oqbn20.prod	apktool_out/lib/arm64-v8a/libelements.so
android-prod-builder@oqbn20.prod	apktool_out/lib/arm64-v8a/libgvr.so
android-prod-builder@oqbn20.prod	apktool_out/lib/arm64-v8a/libgav1JNI.so
android-prod-builder@oqbn20.prod	apktool_out/lib/arm64-v8a/libdrishti_jni_native.so
appro@openssl.org	apktool_out/lib/arm64-v8a/libcronet.93.0.4542.0.so

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312

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

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"password" : "گذرواژه"
"video_privacy_private" : "■■■■■"
"video_privacy_private" : "■■■■■■■■■"
"password" : "Jelszó"
"history_key" : "history_key"
"close_auth_dialog" : "ปิดໜ้าจໍภาบผิสูดยืบยัน"
"video_privacy_private" : "Ιδιωτικό"
"video_privacy_private" : "□□□"
"video_privacy_upload_private_description" : "□□□□□□□"
"publishing_private_video_progress" : "□□□□□□□□□“□□□□□”..."
"password" : "Palavra-passe"
"password" : "■■■■■□■□"
"video_privacy_private" : "Անձնական"

POSSIBLE SECRETS
"password" : "Wachtwoord"
"video_privacy_private" : "Частен"
"video_privacy_private_description" : "ສະເພາະຄົນທີ່ທ່ານເລືອກທີ່ສາມາດເບິ່ງໄດ້"
"accessibility_playlist_private" : "□□□□□□□□□□"
"video_privacy_upload_private_description" : "■■■■■■■■■■■■■■■■■"
"video_privacy_private_description" : "□□□□□□□□□□"
"passive_auth_code_time_out" : "■■■■■■■■■■■■■■■■■■■■■"
"password" : "Heslo"
"password" : "Сырсөз"
"password" : "■■■■■■■■■■■"
"password" : "Zaporka"
"password" : "סיסמה"
"playlist_privacy_private_description" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"accessibility_playlist_private" : "■■■■■■■■■■■"
"close_auth_dialog" : "□□□□□□□□□□"
"video_privacy_private_description" : "□□□□□□□□□□□□□□"
"password" : "Contrasenya"

POSSIBLE SECRETS
"video_privacy_private" : "Privatus"
"auto_play_key" : "auto_play_key"
"password" : "Lösenord"
"video_privacy_private" : "□□□"
"video_privacy_private" : "Şəxsi"
"password" : "□□□□"
"youtube_api_version_name" : "1.12.0"
"video_privacy_private" : "Хувийн"
"premium_early_access_browse_page_key" : "premium_early_access_browse_page_key"
"video_privacy_private" : "Приватно"
"password" : "■■■■■■■"
"playlist_privacy_private_description" : "■■■■■■■■■■■■■■■■■■■"
"video_privacy_private_description" : "□□□□□□□□□□□□"
"video_privacy_private" : "Privát"
"pair_with_tv_key" : "pair_with_tv_key"
"general_key" : "general_key"
"password" : "Aðgangsorð"

POSSIBLE SECRETS
"password" : "Salasana"
"video_privacy_private" : "Privāts"
"playlist_privacy_private_description" : "□□□□□□□□□"
"video_privacy_private" : "■■■■"
"accessibility_playlist_private" : "Pribadi"
"about_key" : "about_key"
"video_privacy_private" : "Privé"
"password" : "Fjalëkalimi"
"accessibility_playlist_private" : "Yksityinen"
"accessibility_playlist_private" : "■■■■■■■■■■■■"
"passive_auth_code_time_out" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"subscription_product_setting_key" : "subscription_product_setting_key"
"video_privacy_upload_private_description" : "□□□□□□□□□"
"accessibility_playlist_private" : "Privélijst"
"password" : "■■■■■■■■"
"password" : "■■■■■■"
"video_privacy_private" : "■■■■■"

POSSIBLE SECRETS
"passive_auth_code_time_out" : "□□□□□□□□□□□□"
"captions_key" : "captions_key"
"video_privacy_private" : "Gizli"
"accessibility_playlist_private" : "Privát"
"parent_tools_key" : "parent_tools_key"
"notification_key" : "notification_key"
"video_privacy_private" : "პირადი"
"connected_accounts_browse_page_key" : "connected_accounts_browse_page_key"
"video_privacy_private" : "Прыватнае"
"video_privacy_private" : "Prywatny"
"video_privacy_private" : "Zaseben"
"password" : "Slaptažodis"
"video_privacy_private" : "Peribadi"
"video_privacy_private" : "Купуя"
"stop_screencast_session_title" : "■■■■■■■■■■■■■■■■■■■■?"
"video_privacy_private" : "■■■■■"
"video_privacy_private" : "■■■■■■■■■"

POSSIBLE SECRETS
"password" : "■■■■■■■■■"
"password" : "Wagwoord"
"password" : "Parol"
"video_privacy_private" : "■■■■■■■■■"
"password" : "□□"
"privacy_key" : "privacy_key"
"video_privacy_private" : "■■■■■"
"offline_key" : "offline_key"
"video_privacy_private" : "■■■■■■□"
"video_privacy_private" : "نجی"
"yt_unplugged_pref_key" : "yt_unplugged_pref_key"
"video_privacy_private" : "■■■■■■"
"password" : "Lozinka"
"password" : "Parool"
"video_privacy_private" : "Pribatua"
"password" : "Nenosiri"
"video_quality_settings_key" : "video_quality_settings_key"

POSSIBLE SECRETS
"accessibility_settings_key" : "accessibility_settings_key"
"close_auth_dialog" : "□□□□□□□□"
"video_privacy_private" : "Privatno"
"password" : "Passord"
"use_password" : "■■■■■■■■■■■■■■■■■■■■■■"
"video_privacy_private" : "Soukromé"
"password" : "Pasahitza"
"password" : "Hasło"
"password" : "Iphasiwedi"
"video_privacy_upload_private_description" : "□□□□□□□□"
"accessibility_playlist_private" : "□□□□□□□"
"third_party_key" : "third_party_key"
"developer_settings_key" : "developer_settings_key"
"video_privacy_private_description" : "□□□□□□□□□□□□□□□□"
"video_privacy_private" : "Private"
"password" : "■■■■■■"
"password" : "Пароль"

POSSIBLE SECRETS
"password" : "Sandi"
"video_privacy_private" : "Pribadi"
"use_password" : "□□□□□□□"
"video_privacy_private" : "Yksityinen"
"video_privacy_private" : "Pribado"
"close_auth_dialog" : "■■■■■■■■■■■■■■■■■■■■■■"
"playlist_privacy_private_description" : "ສະເພາະທ່ານທີ່ເບິ່ງໄດ້"
"close_auth_dialog" : "□□□□□□□□□□□□"
"password" : "□□□□□□"
"video_privacy_private" : "Keke"
"refresh_config_key" : "refresh_config_key"
"video_privacy_upload_private_description" : "ສະເພາະທ່ານທີ່ເບິ່ງໄດ້"
"publishing_private_video_progress" : "□□□□□□□□□□□□□□□□..."
"video_privacy_private" : "Privado"
"password" : "Senha"
"passive_auth_code_time_out" : "ໝົດເວລາຮ້ອງຂໍເຂົ້າສູ່ລະບົບໂທລະທັດ."
"stop_screencast_session_title" : "□□□□□□□□□□□□"

POSSIBLE SECRETS
"playlist_privacy_private_description" : "□□□□□□□"
"password" : "□□"
"yt_unlimited_pre_purchase_key" : "yt_unlimited_pre_purchase_key"
"password" : "Passwort"
"retry_password" : "□□□□□□□□□□□□□□□□“□□□□□”□□□□□□□□"
"password" : "Գաղտնաբառ"
"firebase_database_url" : "https://com--android.firebaseio.com"
"video_privacy_private" : "Imfihlo"
"use_password" : "□□□□□□□"
"password" : "■■■■■■■"
"data_saving_settings_key" : "data_saving_settings_key"
"password" : "პაროლი"
"google_api_key" : "AIzaSyCtkvNIR1HCEwzsqK6JuE6KqpyjusIRl30"
"password" : "Parole"
"video_privacy_private" : "Faragha"
"password" : "■■■■■■■■■"
"video_privacy_private_description" : "■■"

POSSIBLE SECRETS
"video_privacy_private" : "□□□"
"password" : "Parolă"
"stop_screencast_session_title" : "□□□□□□□□□□□□□□□□□□"
"password" : "■■■■■■"
"password" : "ລະຫັດຜ່ານ"
"accessibility_playlist_private" : "□□□□□□□"
"video_privacy_private" : "Lokaď"
"use_password" : "ใส่ละหัดผ่านบับฮิ"
"password" : "Şifre"
"use_password" : "□□□□□□□□□□□□□□□□"
"video_privacy_private" : "خصوصی"
"accessibility_playlist_private" : "ลายกานซั้นส่วนโต"
"video_privacy_private" : "Privée"
"video_privacy_private" : "Privat"
"video_privacy_private" : "Privato"
"passive_auth_code_time_out" : "□□□□□□□□□□□□"
"video_privacy_private" : "Privaatne"

POSSIBLE SECRETS
"playlist_privacy_private_description" : "□□□□□□□□"
"use_password" : "■■■■■■■■■■■■■■■■"
"yt_unlimited_post_purchase_key" : "yt_unlimited_post_purchase_key"
"password" : "Парола"
"live_chat_key" : "live_chat_key"
"password" : "Contraseña"
"video_privacy_private" : "■■■■"
"password" : "Лозинка"
"password" : "Adgangskode"
"video_privacy_private" : "■■■■■■■"
"video_privacy_private" : "Súkromné"
"passive_auth_code_time_out" : "□□□□□□□□□□□□"
"video_privacy_private" : "פרטי"
"password" : "■■■■■■■■■■■■"
"stop_screencast_session_title" : "□□□□□□□□□"
"video_privacy_private" : "ส่วนโต"
"password" : "Password"

POSSIBLE SECRETS
"video_privacy_private" : "خاصّ"
"password" : "Geslo"
"video_privacy_private" : "□□"
"video_privacy_private" : "□□"
"video_privacy_private_description" : "[redacted]"
"password" : "[redacted]"
"passive_auth_code_time_out" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"video_privacy_private" : "Shaxsiy"
"password" : "Contrasinal"
"stop_screencast_session_title" : "[redacted]"
"billing_and_payment_key" : "billing_and_payment_key"
"video_privacy_private" : "□□□"
"stop_screencast_session_title" : "□□□□□□□□"
"close_auth_dialog" : "[redacted]"
"close_auth_dialog" : "□□□□□□□□□"
"video_privacy_upload_private_description" : "[redacted]"
"stop_screencast_session_title" : "ຢຸດການບັນທຶກໜ້າຈໍບໍ?"

POSSIBLE SECRETS
"video_privacy_private" : "Приватне"
"publishing_private_video_progress" : "□□□□□□□□□□□□□□□□□..."
"video_privacy_private" : "■■■■■■■■■■■■"
"google_crash_reporting_api_key" : "AIzaSyCtkvNIR1HCEwzsqK6JuE6KqpyjusIRI30"
"video_privacy_private" : "Privaat"
"dogfood_settings_key" : "dogfood_settings_key"
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
gRg4fCi0LCTpnQrV3PsNLy90ZesL/QRa6YWri3+gAi7rRcznZqsXWOYXHOmcY7vO
C4ABHXMC4Or135sUJAGmAZL7HooHNZP1UfgRABckcZiPz1ZmVgJdnOYsXpFfGNDm
8IixZ0CbQtqPEft6f86OLqdXtqxnPQDWPkO7PVnus4g=
wZfQ+wDgR9IoosBg1su/yp7pQRnlrEzlYNBZbby3s7Z70mOof0UhZ+SwlYLoIxzT
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
Ta7q+IK2mYjuCH0of+Vj0vM5Rtwz8hWo89Z4HIfL3B2t8tHFxG0TQ0Yh0ikc7raQ
enqIddPeKRqzFvVteSKtHxsfYkr9j2sQcVvzi4qN22kodz5l8F1EhNG7Vy+jrIdF
ejLzeiJ5qubwImg6nJzCiB7UFg2tGEG87mpwCGv3DVQ=
O5+El9qd857uJNhBPBY+hYh5U8lug4S2akyjrXXZBPw=
21c8b5470a64adbb25bc84316cbc449361d86839

POSSIBLE SECRETS
49f946663a8deb7054212b8adda248c6
2b12ce565fcbb4ae79851d8324f8396dc908788f-
TiB8Pl2o8LKtvrRgwN2UZPBx2FfVwXaA2LJIyoIsON4gk8JWSfnQXytrQilOHtcO
4/LuQCxE41OF3+ELaCV0AA8Jaj2RFLkgJd6cCnnHOg0=
NW4aS3lNi8fmvEi+Ve4jL+4aAzt/ssbWQU153xX+T2c=
b9XzHrtU52kppUFx5howa5WHGE86IaMftNEAtcnJuYi+uEVxQTZmNq8DYIFxWMDO
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e060355040313 07416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6 96131163014060355040713 0d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e0603550403 1307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372 f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f81 54a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4 dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a3 81d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a 4763074310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e20566965773114301206035504a130b476f 6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e0603550403 1307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a 864886f70d01010405000382010100 6dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0c b109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb 7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7 efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
aBYwH2ThFYuy1U18GzcFTBDhpF5mRbr30vOPELmr1Hc=
G77t423Wv8U+IX+CBfR4k5CGTg8kBFUl+lsHl5zHfM8=
FiLUZy/XwdzoXuv+wZ8fpBUMomrb2qDVGXE0AhvrFclxf2680Tj+s03XL4ZGGoFK

POSSIBLE SECRETS
llqwiPI9WBGdX3ILtNQP0ldd/oo65vCmZGiUmTtHOSQw67bDkVyvEAM6wctf4g5A
ugRDevdIiSCQKB4w29ZHZLzgZXa3WguWUJypfhKkgpE=
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
O8xHH+SQOcjF3BJdz0zTyJmLBvbpWLOG8WSxjEODJJ+MImKFrTu/OMcO8AkFY+Pq
pVEDi4qsv5MtC2dMXzpIaDoRFLsxw
BnUGtdO8J5ukLmkm+ZGsWDuDWstQiBaJlb5Kf+8oxak=
kel/WTUFttZVEFo0c79yp61JugW4yicQRy1hbDIEKZQ=
omAlF62gEMrNCr0H2QBW8XF28QiQE0CMIbyOpElqQZ4tBrxF8DZXvihPhTWIx0tC
AIzaSyC8UYZpvA2eknNex0Pjid0
Wq/IKBdmFHBPtcQG2uw+enxSoneybsCZd6x3sGCEaqo=

POSSIBLE SECRETS
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d01010405003081943 10b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930313233333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d308201203 00d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d01010405000382010010019d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
rfyFxeBVRrcpHOkzoebVIka/58kwozJ0Dt9pVZcWCXE=
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
g3OSAw6b49bJrXDnrxpVD58FlN62AVv4SO1GAfJ7rnU=
cPHMZVY/KwIUfpGqtJoe3sZWjmRLYCJUzedPb6Eusduzq1fr7QzoocP3s4SDqjiP
PpTasJ7rye0SEy8bP+e639N2f2p/VqK1Ye1mnYIaTjk=
DXH16eFlLWYw0RtLAgHDBKxBeg2exJb8qLqayb1oQwo=
4GWYMakWxK9XLQ6iDAU2C2VTll8aRULhAGrQnxilr2Nj0cSsO+IgSBJ8ViB0NlP9
iqnfwKKqiNqrk8VWEttLTKe7o3UJQGSCfPqGJpMmsBc=
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

POSSIBLE SECRETS
3pkKTVgLDXVJJ5N8zGXuZSULCDRtq3PN/ITUaJE7BOs=
115792089210356248762697446949407573529996955224135760342422259061068512044369
c103703e120ae8cc73c9248622f3cd1e
h706sF1zmcc4AioWh+Jfvy0LKoImQxQ7/qBdFNEqjMTCjpxVey9eXR4ewnu7+Xxj
QusX5FxCSt7YALporGf+YBQ7+D9RItA2wCGYVD5mk8FUIvZ7EQ6LwVnumJjBeUBd
e44046539bb5b584279553ca6eacca937c8e16cf
m91XZsk+YhuzWKD4cAkZ4TbV2JwQi634x6I7GtEZSF0=
lJImmJcZfYR8hdrMtfVgK5wxyzq2Tz1kfG0dB54yhkfwwl7Exs4yXjgCxWvlOEKN
B3EEABB8EE11C2BE770B684D95219ECB
rJ0kz5REr7A9K6ozGPC9p0oxIBL7S4eVwdLIqy6EWt/H1xyroUvdpxSKqrgIZI+n
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
115792089210356248762697446949407573530086143415290314195533631308867097853951
GrB7raJKFFs9kqGoJu059MGrbQoaWMXN8wftnS9PR9E=
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
dyzDhPt8uBzEduoVVJNMFQS7AR2KfsUmAWoQzpkryTU=
VkS+X+TtwRpHm8NnTYcac+8VmOK3ly2dr/dAyJrO24Sc1GEe26lkfA2Nk61Ir0mw
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

POSSIBLE SECRETS
ANVavNLSXsNgrppt9T5Uo2JRFQW1glObLu9o
zu63YSe1kidAeMcutkZVGzck9psTtGHz7PCNeED4MwOFY27ac/4JVy5q1i6kfidt
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
wNtnu9iz9FxlWQ/xUwtzm8lbyA6loylNTisLT38FjBA=
9clJleQw8UkEhJcm6dFXqXawxyXf3mRG67a4lWsdtlk=
ciEjxtHwaQq5vQY33BpqQuStjcQqNXynEA7E/ixfFmM=
xAGN8erZZwMSW/Fu3r0voEWCBbBpqzcnOOBzjHGoZvo=
6e2c7e24b7c7eae9fc94882c9f31befa00594872
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
taliwg2sD442czfWRrq8VGyNA1t1bXjQxpcCvWnfA/c=

PLAYSTORE INFORMATION

Title: YouTube

Score: 4.1343718 **Installs:** 10,000,000,000+ **Price:** 0 **Android Version Support:** **Category:** Video Players & Editors **Play Store URL:** com.google.android.youtube

Developer Details: Google LLC, 5700313618786177705, 1600 Amphitheatre Parkway, Mountain View 94043, https://www.youtube.com, ytandroid-support@google.com,

Release Date: Oct 20, 2010 **Privacy Policy:** Privacy link

Description:

Get the official YouTube app on Android phones and tablets. See what the world is watching -- from the hottest music videos to what's popular in gaming, fashion, beauty, news, learning and more. Subscribe to channels you love, create content of your own, share with friends, and watch on any device. Watch and subscribe ● Browse personal recommendations on Home ● See the latest from your favorite channels in Subscriptions ● Look up videos you've watched, liked, and saved for later in Library Explore different topics, what's popular, and on the rise (available in select countries) ● Stay up to date on what's popular in music, gaming, beauty, news, learning and more ● See what's trending on YouTube and around the world on Explore ● Learn about the coolest Creators, Gamers, and Artists on the Rise (available in select countries) Connect with the YouTube community ● Keep up with your favorites creators with Posts, Stories, Premieres, and Live streams ● Join the conversation with comments and interact with creators and other community members Create content from your mobile device ● Create or upload your own videos directly in the app ● Engage with your audience in real time with live streaming right from the app Find the experience that fits you and your family (available in select countries) ● Every family has their own approach to online video. Learn about your options: the YouTube Kids app or a new parent supervised experience on YouTube at youtube.com/myfamily Support creators you love with channel memberships (available in select countries) ● Join channels that offer paid monthly memberships and support their work ● Get access to exclusive perks from the channel & become part of their members community ● Stand out in comments and live chats with a loyalty badge next to your username Upgrade to YouTube Premium (available in select countries) ● Watch videos uninterrupted by ads, while using other apps, or when the screen is locked ● Save videos for when you really need them – like when you're on a plane or commuting ● Get access to YouTube Music Premium as part of your benefits

---

Report Generated by - MobSF v3.9.4 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.