ANDROID STATIC ANALYSIS REPORT

YouTube (16.25.39)

File Name:	YouTube.apk

Package Name:	com.google.android.youtube
Scan Date:	March 11, 2024, 5:16 a.m.
App Security Score:	48/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	INFO	✓ SECURE	HOTSPOT
3	50	0	1	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>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes5.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table></td></tr>
</table>

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

NO	ISSUE	SEVERITY	STANDARDS	FILES

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	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
2	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.
3	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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	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.
5	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
6	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.
7	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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	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.
9	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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	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.
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/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.
13	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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	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.
15	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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	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.
17	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
18	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.
19	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
20	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.
21	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
22	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.
23	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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	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.
25	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
26	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.
27	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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	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.
29	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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
30	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.
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/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.
33	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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
34	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.
35	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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
36	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.
37	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
38	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.
39	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
40	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.

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
www.webrtc.org	ok	**IP:** 64.233.170.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 142.250.4.99 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
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
aomediacodec.github.io	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.youtube.com	ok	**IP:** 172.253.118.190 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
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
symbolize.corp.google.com	ok	**IP:** 74.125.68.129 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
dns.switch.ch	ok	**IP:** 130.59.31.248 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
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
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
support.google.com	ok	**IP:** 172.217.194.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
www.cisco.com	ok	**IP:** 96.16.117.60 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **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
www.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
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
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
dns64.dns.google	ok	No Geolocation information available.
storage.googleapis.com	ok	**IP:** 74.125.24.207 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
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

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
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
public.dns.iij.jp	ok	**IP:** 103.2.57.6 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
developers.google.com	ok	**IP:** 142.251.10.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
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
cleanbrowsing.org	ok	**IP:** 45.77.168.207 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
www.ietf.org	ok	**IP:** 104.16.45.99 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
doh.quickline.ch	ok	**IP:** 212.60.63.246 **Country:** Switzerland **Region:** Bern **City:** Biel **Latitude:** 47.132401 **Longitude:** 7.244110 **View:** Google Map
dns.quad9.net	ok	**IP:** 149.112.112.112 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.796986 **Longitude:** -122.462738 **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
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

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
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
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
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
alekberg.net	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
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

FIREBASE DATABASES

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

EMAILS

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

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

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"passive_auth_code_time_out" : "□□□□□□□□□□□□"
"stop_screencast_session_title" : "■■■■■■■■■■■■■■■■■■■"
"playlist_privacy_private_description" : "ສະເພາະທ່ານທີ່ເບິ່ງໄດ້"
"video_privacy_private" : "Частен"
"video_privacy_private" : "Pribado"
"password" : "■■■■■■■■■"
"video_privacy_private" : "Faragha"
"video_privacy_upload_private_description" : "ສະເພາະທ່ານທີ່ເບິ່ງໄດ້"
"stop_screencast_session_title" : "■■■■■■■■■■■■■■■■■■?"
"password" : "Zaporka"
"video_privacy_private" : "■■■■■■■■■"
"passive_auth_code_time_out" : "□□□□□□□□□□□□"
"password" : "סיסמה"
"premium_early_access_browse_page_key" : "premium_early_access_browse_page_key"
"notification_key" : "notification_key"
"video_privacy_private" : "Pribadi"
"password" : "Fjalëkalimi"

POSSIBLE SECRETS
"pair_with_tv_key" : "pair_with_tv_key"
"close_auth_dialog" : "ປິດໜ້າຈໍການພິສູດຢືນຢັນ"
"use_password" : "□□□□□□□□□□□□□□□"
"live_chat_key" : "live_chat_key"
"video_privacy_private" : "□□"
"password" : "Palavra-passe"
"video_privacy_private" : "■■■■■"
"video_privacy_private" : "Privée"
"dogfood_settings_key" : "dogfood_settings_key"
"video_privacy_private" : "Privatus"
"video_privacy_private" : "Privát"
"video_quality_settings_key" : "video_quality_settings_key"
"video_privacy_private" : "خصوصی"
"password" : "Contrasenya"
"password" : "Slaptažodis"
"passive_auth_code_time_out" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"accessibility_playlist_private" : "■■■■■■■■■■■■"

POSSIBLE SECRETS
"auto_play_key" : "auto_play_key"
"yt_unplugged_pref_key" : "yt_unplugged_pref_key"
"video_privacy_private" : "■■■■■■▯"
"video_privacy_private_description" : "ສະເພາະຄົນທີ່ທ່ານເລືອກທີ່ສາມາດເບິ່ງໄດ້"
"password" : "Passwort"
"video_privacy_private" : "Privé"
"video_privacy_private" : "Soukromé"
"close_auth_dialog" : "▯▯▯▯▯▯▯▯▯"
"video_privacy_private" : "Купуя"
"video_privacy_private" : "Privado"
"close_auth_dialog" : "▯▯▯▯▯▯▯▯▯▯"
"video_privacy_private" : "Privaat"
"password" : "Գաղտնաբառ"
"video_privacy_private" : "Хувийн"
"video_privacy_private" : "Zaseben"
"password" : "Contrasinal"
"yt_unlimited_post_purchase_key" : "yt_unlimited_post_purchase_key"

POSSIBLE SECRETS
"video_privacy_private" : "■■■■"
"general_key" : "general_key"
"video_privacy_private" : "Прыватнае"
"stop_screencast_session_title" : "□□□□□□□□"
"video_privacy_private_description" : "□□□□□□□□□□□"
"video_privacy_private" : "Privat"
"password" : "Heslo"
"playlist_privacy_private_description" : "□□□□□□□"
"use_password" : "■■■■■■■■■■■■■■■■■■■■■■"
"video_privacy_upload_private_description" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"password" : "პაროლი"
"password" : "Lozinka"
"video_privacy_private" : "■■■■■■■■■■■"
"video_privacy_private" : "■■■■■"
"accessibility_playlist_private" : "□□□□□□"
"video_privacy_private" : "■■■■■"
"password" : "Geslo"

POSSIBLE SECRETS
"password" : "Pasahitza"
"password" : "Password"
"video_privacy_private" : "■■■■■"
"video_privacy_private" : "Şəxsi"
"stop_screencast_session_title" : "□□□□□□□□□□□□□"
"stop_screencast_session_title" : "□□□□□□□□"
"use_password" : "■■■■■■■■■■■■■■■■■■■■"
"password" : "■■■■■■■■■"
"subscription_product_setting_key" : "subscription_product_setting_key"
"video_privacy_private" : "Yksityinen"
"video_privacy_private" : "Անձնական"
"password" : "□□"
"password" : "Лозинка"
"video_privacy_private" : "Жеке"
"parent_tools_key" : "parent_tools_key"
"video_privacy_private" : "Shaxsiy"
"use_password" : "□□□□□□□"

POSSIBLE SECRETS
"password" : "■■■■■■■■■"
"accessibility_playlist_private" : "Privát"
"password" : "Senha"
"playlist_privacy_private_description" : "□□□□□□□□"
"stop_screencast_session_title" : "ຢຸດການບັນທຶກໜ້າຈໍບໍ?"
"publishing_private_video_progress" : "□□□□□□□□□□□□□□□..."
"password" : "Contraseña"
"video_privacy_private" : "Ιδιωτικό"
"accessibility_playlist_private" : "□□□□□□□"
"accessibility_playlist_private" : "Yksityinen"
"password" : "Parol"
"video_privacy_private" : "Lokað"
"video_privacy_private" : "□□"
"video_privacy_private" : "ສ່ວນໂຕ"
"password" : "Jelszó"
"accessibility_settings_key" : "accessibility_settings_key"
"video_privacy_private" : "□□□"

POSSIBLE SECRETS
"video_privacy_private" : "Privato"
"video_privacy_private" : "Private"
"stop_screencast_session_title" : "□□□□□□□□□□□□□□□"
"password" : "□□□□□"
"accessibility_playlist_private" : "ລາຍການຫຼິ້ນສ່ວນໂຕ"
"password" : "Parole"
"password" : "Sandi"
"playlist_privacy_private_description" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"password" : "Aðgangsorð"
"password" : "ລະຫັດຜ່ານ"
"accessibility_playlist_private" : "Privélijst"
"passive_auth_code_time_out" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"password" : "■■■■■■■"
"video_privacy_private" : "□□□"
"captions_key" : "captions_key"
"video_privacy_upload_private_description" : "■■■■■■■■■■■■■■■■■"
"password" : "Salasana"

POSSIBLE SECRETS
"password" : "□□□□□□"
"password" : "■■■■■■"
"close_auth_dialog" : "■■■■■■■■■■■■■■■■■■■■■"
"video_privacy_private" : "Privatno"
"close_auth_dialog" : "■■■■■■■■■■■■■■■■■■■■■■■■"
"password" : "■■■■■□■□"
"video_privacy_upload_private_description" : "□□□□□□□"
"video_privacy_private" : "Peribadi"
"video_privacy_private_description" : "□□□□□□□□□"
"billing_and_payment_key" : "billing_and_payment_key"
"use_password" : "□□□□□□"
"video_privacy_private" : "Gizli"
"video_privacy_private" : "Pribatua"
"retry_password" : "□□□□□□□□□□□□□“□□□□”□□□□□□"
"password" : "Lösenord"
"privacy_key" : "privacy_key"
"passive_auth_code_time_out" : "ໝົດເວລາຮ້ອງຂໍເຂົ້າສູ່ລະບົບໂທລະທັດ."

POSSIBLE SECRETS
"video_privacy_private_description" : "□□□□□□□□□□□□"
"password" : "■■■■■■■■■■■"
"close_auth_dialog" : "□□□□□□□"
"password" : "Parolă"
"password" : "Passord"
"video_privacy_private" : "■■■■"
"use_password" : "ໃສ່ລະຫັດຜ່ານບັນຊີ"
"accessibility_playlist_private" : "□□□□□□□□□"
"video_privacy_private" : "نجی"
"passive_auth_code_time_out" : "□□□□□□□□□□"
"video_privacy_private" : "Prywatny"
"video_privacy_private_description" : "■■"
"video_privacy_private_description" : "□□□□□□□□□□□□□□"
"password" : "Parool"
"password" : "Adgangskode"
"video_privacy_private" : "■■■■■■■■■"
"video_privacy_private" : "□□□"

POSSIBLE SECRETS
"publishing_private_video_progress" : "□□□□□□□□□“□□□□□”…"
"accessibility_playlist_private" : "Pribadi"
"video_privacy_private" : "Súkromné"
"password" : "Wachtwoord"
"video_privacy_private" : "■■■■■■■■"
"connected_accounts_browse_page_key" : "connected_accounts_browse_page_key"
"password" : "Wagwoord"
"video_privacy_upload_private_description" : "□□□□□□□"
"firebase_database_url" : "https://com--android.firebaseio.com"
"password" : "Şifre"
"password" : "■■■■■■■■"
"password" : "■■■■■■■■"
"video_privacy_private" : "פרטי"
"video_privacy_private" : "პირადი"
"password" : "■■■■■■■"
"refresh_config_key" : "refresh_config_key"
"accessibility_playlist_private" : "■■■■■■■■■■■■■■■■■"

POSSIBLE SECRETS
"offline_key" : "offline_key"
"video_privacy_private_description" : "■■■■■■■■■■■■■■■■■■■■■■■■"
"video_privacy_private" : "خاصّ"
"password" : "گذرواژه"
"password" : "Hasło"
"publishing_private_video_progress" : "□□□□□□□□□□□□□□□…"
"password" : "Парола"
"google_api_key" : "AIzaSyCtkvNIR1HCEwzsqK6JuE6KqpyjusIRI30"
"video_privacy_private" : "Приватно"
"video_privacy_private" : "Приватне"
"video_privacy_private" : "■■■■■■■■■"
"data_saving_settings_key" : "data_saving_settings_key"
"password" : "■■■■■■"
"video_privacy_private" : "Privāts"
"password" : "Сырсөз"
"yt_unlimited_pre_purchase_key" : "yt_unlimited_pre_purchase_key"
"about_key" : "about_key"

POSSIBLE SECRETS
"video_privacy_private" : "■■■■■■"
"third_party_key" : "third_party_key"
"history_key" : "history_key"
"close_auth_dialog" : "□□□□□□□□□□□□"
"video_privacy_private" : "□□□"
"password" : "Iphasiwedi"
"video_privacy_private" : "Imfihlo"
"passive_auth_code_time_out" : "■■■■■■■■■■■■■■■■■■■■■■■■■"
"playlist_privacy_private_description" : "□□□□□□□□"
"playlist_privacy_private_description" : "■■■■■■■■■■■■■■■■■■■"
"password" : "Nenosiri"
"youtube_api_version_name" : "1.12.0"
"password" : "Пароль"
"password" : "■■■■■■■■■■■■"
"password" : "□□"
"developer_settings_key" : "developer_settings_key"
"google_crash_reporting_api_key" : "AIzaSyCtkvNIR1HCEwzsqK6JuE6KqpyjusIRI30"

POSSIBLE SECRETS
"video_privacy_private" : "Privaatne"
"video_privacy_upload_private_description" : "□□□□□□□□"

PLAYSTORE INFORMATION

Title: YouTube

Score: 4.137572 **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.