MOBSF

ANDROID STATIC ANALYSIS REPORT

YouTube Music (3.69.51)

File Name:	YouTubeMusicPrebuilt.apk
Package Name:	com.google.android.apps.youtube.music
Scan Date:	March 19, 2024, 5:49 a.m.

App Security Score:	49/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	32	2	2	1

FILE INFORMATION

File Name: YouTubeMusicPrebuilt.apk
Size: 35.33MB
MD5: 1c5ffd8fe9ba7502db55167321404d2e
SHA1: 91a1ff59b38131ff0c1075c536dff1ea1b3505e9
SHA256: b4c168e5db6d9ca257c25d608a6089b85c275a49c4d0fddd6fad43be185280f0

APP INFORMATION

App Name: YouTube Music
Package Name: com.google.android.apps.youtube.music
Main Activity: com.google.android.apps.youtube.music.activities.MusicActivity
Target SDK: 29
Min SDK: 21
Max SDK:
Android Version Name: 3.69.51
Android Version Code: 36951240

APP COMPONENTS

Activities: 15
Services: 13
Receivers: 24
Providers: 3
Exported Activities: 5
Exported Services: 3
Exported Receivers: 9
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=California, L=Mountain View, O=Google Inc., OU=Android, CN=ytmusic
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-10-10 19:18:10+00:00
Valid To: 2042-02-25 19:18:10+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=ytmusic
Serial Number: 0xa1243b67d0205a71

Hash Algorithm: sha1
md5: 48042f18b7070092ff80dc1a921ccfbd
sha1: afb0fed5eeaebdd86f56a97742f4b6b33ef59875
sha256: a2a1ad7ba7f41dfca4514e2afeb90691719af6d0fdbed4b09bbf0ed897701ceb
sha512: 2866bb944318b8d3b7927e770015830367757ebf84c80b9916ab434342235e79bf154891d758960f0aa6d1913bba72a48d3362c92a34a70ea9ae60fb11c84f12
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b791dadaea00f0be652d6d6be30a7b654c5d563f6ba21a123339ff8ad403f405
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
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.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>/home/mobsf/.MobSF/uploads/1c5ffd8fe9ba7502db55167321404d2e/1c5ffd8fe9ba7502db55167321404d2e.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></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</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</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.MODEL check
Build.MANUFACTURER check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes4.dex	FINDINGS: Compiler — DETAILS: r8

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.google.android.apps.youtube.music.activities.MusicActivity	Schemes: vnd.youtube.music://, vnd.youtube.music.launch://,
com.google.android.apps.youtube.music.audiopreview.AudioPreviewPlayerActivity	Schemes: file://, http://, https://, content://, Mime Types: audio/*, application/ogg, application/x-ogg, application/itunes,
com.google.android.apps.youtube.music.deeplink.MusicServiceDeepLinkActivity	Schemes: http://, https://, Hosts: music.youtube.com, www.music.youtube.com, m.music.youtube.com, music.youtu.be, music.youtube, yt.be, Path Patterns: .*, /music/.*,

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.
3	youtube.com googleapis.com	secure	Domain config is securely configured to disallow clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 2 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **19** | INFO: **0** | SUPPRESSED: **0**

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.
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.apps.youtube.music.offline.OfflineStorePackageReplacedReceiver) 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.
5	Activity (com.google.android.apps.youtube.music.activities.MusicPickerActivity) 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.
6	Activity (com.google.android.apps.youtube.music.audiopreview.AudioPreviewPlayerActivity) 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
7	TaskAffinity is set for activity (com.google.android.apps.youtube.music.deeplink.MusicServiceDeepLinkActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
8	Activity (com.google.android.apps.youtube.music.deeplink.MusicServiceDeepLinkActivity) 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	Broadcast Receiver (androidx.media.session.MediaButtonReceiver) 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.
10	Service (com.google.android.apps.youtube.music.mediabrowser.MusicBrowserService) 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.
11	Broadcast Receiver (com.google.android.apps.youtube.music.mediabrowser.waze.MusicWazeBroadcastReceiver) 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.
12	Service (com.google.android.apps.youtube.music.notifications.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.
13	Broadcast Receiver (com.google.android.libraries.youtube.account.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.
14	Broadcast Receiver (com.google.android.apps.youtube.music.player.widget.MusicWidgetProvider) 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.
15	Broadcast Receiver (com.google.android.apps.youtube.music.player.widget.PendingIntentReceiver) 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.
16	Broadcast Receiver (com.google.android.libraries.phenotype.client.stable.PhenotypeStickyAccount$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.
17	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.

NO	ISSUE	SEVERITY	DESCRIPTION
18	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.
19	Activity (androidx.biometric.DeviceCredentialHandlerActivity) 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.
20	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.
21	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: **1** | WARNING: **8** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/makeramen/RoundedImageView.java defpackage/aaed.java defpackage/aaeg.java defpackage/aaen.java defpackage/aafe.java defpackage/aagi.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/aahq.java defpackage/aaii.java defpackage/aais.java defpackage/aait.java defpackage/aaiz.java defpackage/aajf.java defpackage/aajg.java defpackage/aajh.java defpackage/aaji.java defpackage/aajl.java defpackage/aajs.java defpackage/aajx.java defpackage/aakp.java defpackage/aakx.java defpackage/aale.java defpackage/aalg.java defpackage/aall.java defpackage/aalx.java defpackage/aaly.java defpackage/aalz.java defpackage/aamf.java defpackage/aamg.java defpackage/aamk.java defpackage/aba.java defpackage/abq.java defpackage/ach.java defpackage/ada.java defpackage/adr.java defpackage/aev.java defpackage/afj.java defpackage/afl.java defpackage/afp.java defpackage/afs.java defpackage/aft.java defpackage/afv.java defpackage/afx.java defpackage/agi.java defpackage/ahc.java defpackage/akxk.java defpackage/akxn.java defpackage/akxq.java defpackage/akxr.java defpackage/akxs.java defpackage/akxv.java defpackage/akxw.java defpackage/akxz.java defpackage/akym.java defpackage/akys.java defpackage/akyu.java defpackage/akzv.java defpackage/albp.java defpackage/albq.java defpackage/aldy.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/alq.java defpackage/alt.java defpackage/alts.java defpackage/amf.java defpackage/aml.java defpackage/amv.java defpackage/ande.java defpackage/anfc.java defpackage/anhg.java defpackage/anhw.java defpackage/anhx.java defpackage/anhy.java defpackage/anid.java defpackage/anio.java defpackage/anr.java defpackage/ant.java defpackage/anu.java defpackage/anv.java defpackage/anw.java defpackage/any.java defpackage/anz.java defpackage/aoc.java defpackage/aor.java defpackage/aou.java defpackage/ape.java defpackage/apl.java defpackage/apr.java defpackage/apw.java defpackage/ara.java defpackage/arp.java defpackage/ars.java defpackage/arv.java defpackage/arz.java defpackage/aue.java defpackage/aux.java defpackage/ayy.java defpackage/az.java defpackage/azu.java defpackage/bbe.java defpackage/bbo.java defpackage/bi.java defpackage/bj.java defpackage/bjn.java defpackage/bkh.java defpackage/blu.java defpackage/bqm.java defpackage/br.java defpackage/brb.java defpackage/brm.java defpackage/btt.java defpackage/bu.java defpackage/bvw.java defpackage/bvz.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/bw.java defpackage/bxm.java defpackage/bxv.java defpackage/byi.java defpackage/byp.java defpackage/bys.java defpackage/byw.java defpackage/bzu.java defpackage/cat.java defpackage/ccm.java defpackage/cdi.java defpackage/cdk.java defpackage/cel.java defpackage/cjo.java defpackage/cxk.java defpackage/cze.java defpackage/czh.java defpackage/czm.java defpackage/czn.java defpackage/dde.java defpackage/dfw.java defpackage/dz.java defpackage/fa.java defpackage/fc.java defpackage/fmc.java defpackage/fnh.java defpackage/fnm.java defpackage/fno.java defpackage/fnp.java defpackage/ftu.java defpackage/fup.java defpackage/fuq.java defpackage/fve.java defpackage/fxi.java defpackage/fz.java defpackage/gb.java defpackage/ghh.java defpackage/hd.java defpackage/hqq.java defpackage/hqu.java defpackage/hrt.java defpackage/hsm.java defpackage/htp.java defpackage/hus.java defpackage/hvc.java defpackage/hwy.java defpackage/hxb.java defpackage/hxc.java defpackage/hxw.java defpackage/hzk.java defpackage/hzt.java defpackage/hzu.java defpackage/iap.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	defpackage/iay.java defpackage/ibu.java defpackage/icr.java defpackage/icz.java defpackage/ige.java defpackage/iib.java defpackage/ija.java defpackage/ijc.java defpackage/ijn.java defpackage/ijp.java defpackage/ijr.java defpackage/ikh.java defpackage/ikk.java defpackage/ikv.java defpackage/ino.java defpackage/ioz.java defpackage/irh.java defpackage/irx.java defpackage/it.java defpackage/itc.java defpackage/itd.java defpackage/iug.java defpackage/iuh.java defpackage/ium.java defpackage/ius.java defpackage/iw.java defpackage/iwl.java defpackage/iyt.java defpackage/izn.java defpackage/izy.java defpackage/jam.java defpackage/jbm.java defpackage/jc.java defpackage/jdq.java defpackage/jea.java defpackage/jg.java defpackage/jgv.java defpackage/jko.java defpackage/jpx.java defpackage/jrz.java defpackage/js.java defpackage/jsu.java defpackage/jtk.java defpackage/jtl.java defpackage/jto.java defpackage/jtu.java defpackage/jtv.java defpackage/juc.java defpackage/jud.java defpackage/juv.java defpackage/jwe.java defpackage/jwk.java defpackage/jxa.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/jxe.java defpackage/jxh.java defpackage/jxm.java defpackage/jxv.java defpackage/jxx.java defpackage/jxz.java defpackage/jy.java defpackage/jzd.java defpackage/kaf.java defpackage/kai.java defpackage/kal.java defpackage/kan.java defpackage/kau.java defpackage/kba.java defpackage/kbb.java defpackage/kbh.java defpackage/kbk.java defpackage/kbl.java defpackage/kbp.java defpackage/kcb.java defpackage/kcc.java defpackage/kcw.java defpackage/kcy.java defpackage/kdd.java defpackage/kdq.java defpackage/kdx.java defpackage/kgk.java defpackage/khb.java defpackage/khf.java defpackage/kia.java defpackage/kin.java defpackage/kio.java defpackage/kiv.java defpackage/kjb.java defpackage/kjc.java defpackage/kjd.java defpackage/klm.java defpackage/kln.java defpackage/klo.java defpackage/klp.java defpackage/klq.java defpackage/klr.java defpackage/klt.java defpackage/klv.java defpackage/klz.java defpackage/kmz.java defpackage/ko.java defpackage/kpc.java defpackage/kqb.java defpackage/kqu.java defpackage/krr.java defpackage/kt.java defpackage/kv.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/kw.java defpackage/kx.java defpackage/kxp.java defpackage/ky.java defpackage/le.java defpackage/lev.java defpackage/lf.java defpackage/lh.java defpackage/ljt.java defpackage/lki.java defpackage/lkr.java defpackage/ll.java defpackage/lnp.java defpackage/ls.java defpackage/ltc.java defpackage/lur.java defpackage/lvj.java defpackage/lvk.java defpackage/lvm.java defpackage/lvz.java defpackage/lwc.java defpackage/lwl.java defpackage/lx.java defpackage/lyy.java defpackage/mcb.java defpackage/mcg.java defpackage/mem.java defpackage/mep.java defpackage/mle.java defpackage/mli.java defpackage/mlm.java defpackage/mrc.java defpackage/mvx.java defpackage/mwc.java defpackage/mz.java defpackage/nd.java defpackage/ng.java defpackage/nit.java defpackage/nja.java defpackage/njc.java defpackage/njd.java defpackage/njj.java defpackage/njk.java defpackage/njl.java defpackage/njn.java defpackage/njx.java defpackage/nk.java defpackage/nka.java defpackage/nkp.java defpackage/nks.java defpackage/nmi.java defpackage/nq.java defpackage/nqp.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/nrv.java defpackage/nsq.java defpackage/nst.java defpackage/nsw.java defpackage/ntd.java defpackage/nyl.java defpackage/obg.java defpackage/pkt.java defpackage/pse.java defpackage/pth.java defpackage/pu.java defpackage/qde.java defpackage/qhl.java defpackage/qhs.java defpackage/ql.java defpackage/qn.java defpackage/qw.java defpackage/ro.java defpackage/rq.java defpackage/ryu.java defpackage/sno.java defpackage/tia.java defpackage/tpy.java defpackage/tw.java defpackage/uik.java defpackage/vi.java defpackage/vn.java defpackage/we.java defpackage/xe.java defpackage/xf.java defpackage/xil.java defpackage/yc.java defpackage/ylo.java defpackage/yqm.java defpackage/yrl.java defpackage/yrw.java defpackage/ysx.java defpackage/ytk.java defpackage/zlf.java defpackage/zlu.java defpackage/zly.java defpackage/zy.java
				defpackage/bh.java defpackage/jak.java defpackage/jal.java defpackage/ksk.java defpackage/kso.java defpackage/ksx.java defpackage/ksy.java defpackage/kxj.java defpackage/lcs.java defpackage/lcw.java defpackage/lmj.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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/lml.java defpackage/lnx.java defpackage/lny.java defpackage/nxs.java defpackage/nyh.java defpackage/ocy.java defpackage/ocz.java defpackage/oda.java defpackage/odb.java defpackage/odc.java defpackage/odd.java defpackage/psk.java defpackage/psl.java defpackage/pso.java defpackage/uhl.java defpackage/usl.java defpackage/uwd.java defpackage/uxz.java defpackage/uyn.java defpackage/uyp.java defpackage/uyq.java defpackage/uyr.java defpackage/uys.java defpackage/uyt.java defpackage/uyu.java defpackage/uyv.java defpackage/uyw.java defpackage/uyx.java defpackage/uyy.java defpackage/uyz.java defpackage/uza.java defpackage/uzb.java defpackage/uzc.java defpackage/uzd.java defpackage/uze.java defpackage/uzf.java defpackage/uzg.java defpackage/uzh.java defpackage/uzi.java defpackage/uzj.java defpackage/uzk.java defpackage/uzl.java defpackage/uzm.java defpackage/uzn.java defpackage/uzo.java defpackage/uzp.java defpackage/uzr.java defpackage/uzs.java defpackage/uzt.java defpackage/uzu.java defpackage/uzv.java defpackage/uzx.java defpackage/uzy.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/vap.java defpackage/vle.java defpackage/aaeq.java defpackage/alxa.java defpackage/alxd.java defpackage/alxg.java defpackage/ambw.java defpackage/amdv.java defpackage/cwc.java defpackage/cxk.java defpackage/hzu.java defpackage/iap.java defpackage/ine.java defpackage/iws.java defpackage/izc.java defpackage/kgl.java defpackage/ldc.java defpackage/llt.java defpackage/nbz.java defpackage/nic.java defpackage/osm.java defpackage/ovv.java defpackage/ovx.java defpackage/qhd.java defpackage/qxg.java defpackage/taj.java defpackage/thl.java defpackage/tof.java defpackage/uci.java defpackage/wwu.java defpackage/xjp.java defpackage/yyd.java defpackage/zbs.java defpackage/zbt.java defpackage/zbu.java j$/util/concurrent/ThreadLocalRandom.java
4	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/aakq.java defpackage/alio.java defpackage/deo.java defpackage/kiv.java
5	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	defpackage/aliq.java defpackage/dep.java defpackage/qka.java defpackage/sax.java defpackage/sbb.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/aaii.java defpackage/aakp.java defpackage/akys.java defpackage/aljf.java defpackage/egw.java defpackage/nqp.java defpackage/qkb.java defpackage/uhy.java defpackage/wss.java defpackage/xiz.java
7	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/cwq.java
8	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/akxv.java defpackage/jw.java defpackage/ntg.java defpackage/qhe.java defpackage/vde.java defpackage/vjv.java defpackage/vlx.java
9	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/hok.java defpackage/ocx.java
10	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/cvi.java defpackage/ixz.java defpackage/ldc.java defpackage/mrp.java defpackage/mwz.java defpackage/nyv.java
11	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/att.java defpackage/dpi.java defpackage/wdf.java
12	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	defpackage/njc.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	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
2	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: ['__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	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
4	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: ['__vsnprintf_chk', '__read_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/libcronet.84.0.4128.0.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: ['__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__FD_SET_chk', '__FD_ISSET_chk', '__FD_CLR_chk']	False warning Symbols are available.

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	arm64-v8a/libwebp_android.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
9	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.	$ORIGIN/../../../../../../../../../_solib_arm64-v8a/_U_S_Sthird_Uparty_Slibvpx_Cvpx_Uandroid_Ushared_Uarm64-v8a_Uhighbd___Uthird_Uparty_Slibvpx_Slibs_Sdefault_Shighbd_Sarm64-v8a high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler option --enable-new-dtags,-rpath to remove RUNPATH.	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/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: ['__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	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.	$ORIGIN/../../../../../../_solib_arm64-v8a/_U_S_Sthird_Uparty_Slibvpx_Cvpx_Uandroid_Ushared_Uarm64-v8a_Uhighbd___Uthird_Uparty_Slibvpx_Slibs_Sdefault_Shighbd_Sarm64-v8a high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler option --enable-new-dtags,-rpath to remove RUNPATH.	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
12	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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
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/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: ['__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	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
16	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: ['__vsnprintf_chk', '__read_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	arm64-v8a/libcronet.84.0.4128.0.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: ['__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__FD_SET_chk', '__FD_ISSET_chk', '__FD_CLR_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	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
19	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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	arm64-v8a/libwebp_android.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
21	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.	$ORIGIN/../../../../../../../../../_solib_arm64-v8a/_U_S_Sthird_Uparty_Slibvpx_Cvpx_Uandroid_Ushared_Uarm64-v8a_Uhighbd___Uthird_Uparty_Slibvpx_Slibs_Sdefault_Shighbd_Sarm64-v8a high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler option --enable-new-dtags,-rpath to remove RUNPATH.	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/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: ['__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	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.	$ORIGIN/../../../../../../_solib_arm64-v8a/_U_S_Sthird_Uparty_Slibvpx_Cvpx_Uandroid_Ushared_Uarm64-v8a_Uhighbd___Uthird_Uparty_Slibvpx_Slibs_Sdefault_Shighbd_Sarm64-v8a high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler option --enable-new-dtags,-rpath to remove RUNPATH.	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
24	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
Malware Permissions	12/24	android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.SYSTEM_ALERT_WINDOW, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.GET_ACCOUNTS, android.permission.ACCESS_FINE_LOCATION, android.permission.RECORD_AUDIO

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	5/45	android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.ACTIVITY_RECOGNITION, 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
www.google.com	ok	**IP:** 74.125.200.106 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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

DOMAIN	STATUS	GEOLOCATION
m.youtube.com	ok	**IP:** 172.253.118.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
youtube.com	ok	**IP:** 142.251.175.91 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developers.cloudflare.com	ok	**IP:** 104.16.6.189 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
goo.gl	ok	**IP:** 142.251.12.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
dns10.quad9.net	ok	**IP:** 9.9.9.10 **Country:** United States of America **Region:** California **City:** Berkeley **Latitude:** 37.879318 **Longitude:** -122.265205 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebase.google.com	ok	**IP:** 142.251.175.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.googleadservices.com	ok	**IP:** 74.125.130.154 **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:** 172.217.194.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
dummy.googlevideo.com	ok	No Geolocation information available.
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
release-youtubei.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

DOMAIN	STATUS	GEOLOCATION
support.google.com	ok	**IP:** 74.125.68.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
suggestqueries.google.com	ok	**IP:** 74.125.68.138 **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
app-measurement.com	ok	**IP:** 74.125.24.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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

DOMAIN	STATUS	GEOLOCATION
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
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
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
play.google.com	ok	**IP:** 64.233.170.102 **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

DOMAIN	STATUS	GEOLOCATION
pagead2.googlesyndication.com	ok	**IP:** 172.217.194.154 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
cami-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
s.youtube.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
developers.google.com	ok	**IP:** 64.233.170.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
plus.google.com	ok	**IP:** 74.125.200.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

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
imasdk.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
googleads.g.doubleclick.net	ok	**IP:** 142.251.175.155 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
csi.gstatic.com	ok	**IP:** 142.250.126.120 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
dns11.quad9.net	ok	**IP:** 9.9.9.11 **Country:** United States of America **Region:** California **City:** Berkeley **Latitude:** 37.879318 **Longitude:** -122.265205 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
myaccount.google.com	ok	**IP:** 172.253.118.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google-analytics.com	ok	**IP:** 64.233.170.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
upload.youtube.com	ok	**IP:** 142.251.12.116 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
chrome.cloudflare-dns.com	ok	**IP:** 172.64.41.3 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
dns.google	ok	**IP:** 8.8.4.4 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ssl.google-analytics.com	ok	**IP:** 74.125.200.97 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.googleapis.com	ok	**IP:** 74.125.24.95 **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.
www.youtube	ok	No Geolocation information available.
test-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
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
www.googletagmanager.com	ok	**IP:** 142.250.4.97 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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
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
metal-dimension-646.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.youtube.com	ok	**IP:** 74.125.68.136 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.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
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
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:** 142.251.10.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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

DOMAIN	STATUS	GEOLOCATION
maps.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
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.gstatic.com	ok	**IP:** 64.233.170.94 **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:** 45.79.19.196 **Country:** United States of America **Region:** Texas **City:** Richardson **Latitude:** 32.948181 **Longitude:** -96.729721 **View:** Google Map
green-youtubei.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

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://metal-dimension-646.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	defpackage/jts.java
tu_promo_dialog_logo@2x.png tu_promo_dialog_logo@3x.png	Android String Resource
android-prod-builder@oxtz12.prod	lib/arm64-v8a/libgvr_audio.so
appro@openssl.org android-prod-builder@oxtz12.prod	lib/arm64-v8a/libelements.so
android-prod-builder@oxtz12.prod	lib/arm64-v8a/libgvr.so
appro@openssl.org	lib/arm64-v8a/libcronet.84.0.4128.0.so
android-prod-builder@oxtz12.prod	apktool_out/lib/arm64-v8a/libgvr_audio.so
appro@openssl.org android-prod-builder@oxtz12.prod	apktool_out/lib/arm64-v8a/libelements.so
android-prod-builder@oxtz12.prod	apktool_out/lib/arm64-v8a/libgvr.so
appro@openssl.org	apktool_out/lib/arm64-v8a/libcronet.84.0.4128.0.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
"playlist_privacy_private" : "Прыватны"
"playlist_privacy_private" : "Pribado"
"playlist_privacy_private" : "Soukromý"
"playlist_privacy_private" : "Pribatua"
"playlist_privacy_private" : "Peribadi"
"playlist_privacy_private" : "Privaat"
"playlist_privacy_private" : "Pribadi"
"playlist_privacy_private" : "Privatus"
"playlist_privacy_private" : "Particular"
"playlist_privacy_private" : "■■■■■■□"
"playlist_privacy_private" : "Ιδιωτικό"
"firebase_database_url" : "https://metal-dimension-646.firebaseio.com"
"playlist_privacy_private" : "□□□"
"playlist_privacy_private" : "Privatni"
"playlist_privacy_private" : "Shaxsiy"
"playlist_privacy_private" : "Privatno"

POSSIBLE SECRETS
"playlist_privacy_private" : "Privata"
"playlist_privacy_private" : "პირადი"
"playlist_privacy_private" : "[redacted]"
"playlist_privacy_private" : "Privat"
"playlist_privacy_private" : "Şəxsi"
"playlist_privacy_private_detail" : "[redacted]"
"playlist_privacy_private" : "Prywatna"
"playlist_privacy_private" : "[redacted]"
"playlist_privacy_private" : "[redacted]"
"playlist_privacy_private" : "Lokaður"
"google_crash_reporting_api_key" : "AIzaSyAOghZGza2MQSZkY_zfZ370N-PUdXEo8AI"
"playlist_privacy_private" : "Privát"
"playlist_privacy_private" : "Eyimfihlo"
"playlist_privacy_private" : "Privé"
"playlist_privacy_private" : "[redacted]"
"playlist_privacy_private" : "[redacted]"
"playlist_privacy_private" : "Privāts"
"playlist_privacy_private" : "Անձնական"
"playlist_privacy_private" : "[redacted]"
"playlist_privacy_private_detail" : "[redacted]"

POSSIBLE SECRETS
"playlist_privacy_private" : "Частен"
"playlist_privacy_private" : "Gizli"
"playlist_privacy_private" : "Приватний"
"playlist_privacy_private" : "□□"
"playlist_privacy_private" : "■■■■■■"
"playlist_privacy_private" : "■■■■■"
"google_api_key" : "AIzaSyAOghZGza2MQSZkY_zfZ370N-PUdXEo8AI"
"playlist_privacy_private" : "خصوصی"
"playlist_privacy_private_detail" : "□□□□□□□□"
"playlist_privacy_private" : "■■■■"
"playlist_privacy_private" : "Privatna"
"playlist_privacy_private" : "etavirP"
"playlist_privacy_private_detail" : "□□□□□□□□□□"
"playlist_privacy_private" : "Private"
"playlist_privacy_private" : "■■■■■"
"playlist_privacy_private" : "■ ■■■■■"
"playlist_privacy_private" : "Жеке"
"playlist_privacy_private" : "نجی"
"playlist_privacy_private_detail" : "□□□□□□□□□"
"playlist_privacy_private" : "Zaseben"

POSSIBLE SECRETS
"playlist_privacy_private" : "Хувийн"
"playlist_privacy_private" : "خاصة"
"playlist_privacy_private" : "Yksityinen"
"playlist_privacy_private" : "□□□"
"playlist_privacy_private" : "■■■■■■■■■"
"playlist_privacy_private" : "פרטי"
"playlist_privacy_private" : "Купуя"
"playlist_privacy_private" : "■■■■■■■■■"
"playlist_privacy_private" : "Приватна"
"playlist_privacy_private_detail" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"playlist_privacy_private" : "ส่วนตัว"
"playlist_privacy_private" : "Privaatne"
"playlist_privacy_private_detail" : "ສະເພາະຫ່ານທີ່ເບິ່ງໄດ້"
"playlist_privacy_private" : "Privée"
"playlist_privacy_private" : "Súkromný"
"playlist_privacy_private" : "■■■■"
"playlist_privacy_private" : "Privada"
mLW4WfBtN0b1ZboDT/Xcg0iQ140V7G6lHXVBVeBNgLy2jqsT86h2d5npN9bwHugA
yc8yVBGvbM+lDFTeqeGtXc4ZNvehxfgG+5lUS0qb9Du8+QB2SPf9wsrUE/z4yk8S
ECBqiWBAFfHVW9c0fNISGmIVHjwqX6w+ErcYZElUmEc=

POSSIBLE SECRETS
0LbfErERsnzVecZdFdN1r+gkwDj0UWKblMs3MLLnL2Xbg6jOw+rQN6l6e1wPHG33
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186160697311231 9
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
BgRtXwp/TdPjOMTtxgPOZvXLI0QBLAqNFbcCQtGyZIw=
JvvFzwwo66S0VRYmvytx5jLGWNK4QTG9DsWMC8EHPsa+dy60MhFDXxhSCFeMdBUA
zX3km1qPLrYiG9n7dUoZFQC+zmTqD3abHbpkWV6m20n4Hps2FMxcbSPgd5Hww3wz
21c8b5470a64adbb25bc84316cbc449361d86839
JRUkDJhW1HFHNphIghrQ/GpgsHAYhKZrP+QjqJGAwmK1uoDv5DksWYPGE3Clg8Wl
3iWeLGlh18NsDExlN2QlzTmA4vWzzS1+BPse+PPBjp4=
zr0B6w2ARZzNLj2nzDGif7orJvzwcPV/ZAvZlkxUu58=
rSYhJJHF5kuUSeVTNPNw2nZQeRBUWQY9GRiatfzsnBI=
UQKiPRoyS+CnmUD46E4EQsdx5KAVcG8QUHzjpjKV7eOLJZ8IiejnQxha3R+ewm0b
D8c6NAmywhfnShC87wKLOPWI667JyTy6/R+sj2OrkcE=
7PTXHfesCwrygeE6a5SpFPYapA+6N5AjzCxH/Yeev9s=
eNJuSXkridnHpFkTgNBQFH0ivDH801goaJfT5bONEac=
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
XLHOfrBefh/XuKTLTjyhlPIaCxluS3pTQi+gEZfTBluRJuWX3xNYXE2jLxpQRzgB
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
DL06yVystRGRjM8EyvmOgS0+0UCTDIf3AO1BdC6S2Xc=
YNaCscR40XE3jUfiuSQHOi4SzYzHuKIdiPgG8VTOtns=

POSSIBLE SECRETS
xbfft456rqtoEjzflxINvm3jB0UueLr4QkvjRWQER1VwL7sPWXVbi0ERv76eXFyQ
A9PMpBtOrhEBwg8EX+pCzRKXDVxnOl4pjePaLvko3/E=
S7j7LD+X97hW9j19Wlw8PL4uee7GXfPlwR/necYXNzsTAuZoEKTwM2kjDqHm05Xn
Mg7hpNILFKkl7hAkw7A/iVut8RlgxPSTSSiW9E7s4cWD5OqGx03LJQgW7i+QM0lp
jgvEncvxob+pdE8d4JYFj2otUJMxUVgOSjZFi7SPhb8=
1bR3VLwyKPqduFBz9kXnGy9UPty9HeyYL7t+HjE4ync=
ml4AvGY+nQt22tJsUNFln/OBC0y4peiX+clO3RuuvHbZxKoMDV9bJ0uZQRoWlvUW
cf029002fffdcadf079e8d0a1c9a70ac
43eOblbU7A9iaWARuDVFJ8N1XD9E6UlUqKostw/+hyU=
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
6MSHSlSyck9tPP3AhA1TvP6GMucaxnzE6fuqtUKNFpo3t/1gZkhYdWZ3T7TqgVQ+
ReoS3B5WMCMFdJKmPyF5hDrYSl+H3suOGmd1TWj29uY=
KPLQ0fePjwRZEMYpyhf3z9wME5WAXo6nyi3l+jJDepzY4MR9ieVKu+2i7JuNsveg
ZYG1jdm5AM7mUcEoXCq3rK65rJCTC1sw09mQRjZNz08G/w3QyVfe+O2dWBpXFfYE
6tksJC1oiOeEiy2PbP6Xt59/bZLk2jiIwJLpwcxJtmo=
Gi2YikSW4mz4yLeV51PuRFzLB4uKpJt5dlUqD2L9JzjHJ007dtZdVfKWEzHFdZMW
e44046539bb5b584279553ca6eacca937c8e16cf
VmyCEaBbgXUge3crX5DhhnNRVJcJLKw2o+4M6cwlJJA=
26Ohttc1YMDS/slW8vGpdK8iFLV040F3RgiqDCo8vCY=

POSSIBLE SECRETS
ceQUDMmIspNePIQJbm5sD+0WYMcJxKiy+KS8DogRZko=
PodJLO62QvFjTRyT1s1j7Q9gO2vYuekX/f9fSujDgK0lEz9+ovbaOYnK8KkglxI5
Z7KH49fR2DjGspeuHX8BcHTD0uvOOHknJOx30FGv58BpyVtvGyvjuMhyW8cRn2RI
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
X0m24tw9RfpfSH/8tn2SLvPJTtxlpwlibbKYTkjQXto=
Q2/dQoYza3Uuw12qqlI5Okt59+FCPCwuUEpf8JYT3zQ=
2674cc2dc151f143d20e8d7f7dfc01851f2c87de-
TkuK+8ZKbIcxeUe4msY7eeifKf/tICuqqRvwzwQUhsKM0HemvJhBrPQYp0qpvgcE
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
2pYopzTvTKz5lKmw9xOg8KoJpRi+qonTMAPEuw8ei1o=
oGPxyK0MwPjhYamik95TRAfpfH6vWsbKtfhXi+EQnuc=
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
17DwGTsvrSwrOOIos7QWdg74ixLWLGA2Yzsqu+WYLrw=
F/EU4ZcvKrJZHhJGs54afTSYBM9roD2BTsVzFmIfQmM=
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
fJGzXKpU2C8iDl+Y7ANdP7v6dQ4TyTGpRfe+tJE9nXBQ6AkONmMJiKZGUd7krHwa

POSSIBLE SECRETS
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
AIzaSyCbNu0kKlAVm5mL6m4NUEgCUl0NR3nPqLs
Cr3Y6+GncptpU6DnnTxAUgghcXzA5hROF2y+XKP1eRU=
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
6e2c7e24b7c7eae9fc94882c9f31befa00594872
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
8aff2efc47fafe870c738f727dfcfc6e

PLAYSTORE INFORMATION

Title: YouTube Music

Score: 4.436031 **Installs:** 1,000,000,000+ **Price:** 0 **Android Version Support:** **Category:** Music & Audio **Play Store URL:** com.google.android.apps.youtube.music

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

Release Date: Nov 12, 2015 **Privacy Policy:** Privacy link

Description:

Connecting you to the world of music: ● More than 100 million official songs ● Music content including live performances, covers, remixes and music content you can't find elsewhere ● Thousands of curated playlist across many genres and activities Get personalized music, perfect for every moment: ● Personalized playlists and Mixes made just for you, built around your favorite types of music ● Personalized activity mixes for your Workout, Relax, and Focus sessions ● Create playlists with song suggestions or collaborate with other music fans to create the perfect playlist ● Personalized Library to see all of your liked and added songs, playlists, artists, and albums Stay on top of the trend and discover new music: ● Check out curated for you mixes such Discover Mix and New Release Mix ● Discover music based genres (Hip Hop, Pop, Country, Dance & Electronic, Blues, Indie & Alternative, Jazz, Kpop, Latin, Rock, and more) ● Discover music based mood (Chill, Feel Good, Energy Booster, Sleep, Focus, Romance, Workout, Commute, Party) ● Explore top charts from all over the world Enhanced your listening experience with unique features: ● Song lyrics so you can sing along to your favorites ● Switch seamlessly between audio and video ● Listen on your phone, desktop, smart speaker, smart TV, car, smart watch and within your favorite apps. ● Add a Tile on your Wear OS watch to quickly access your music. ● Compatible with Google Maps, Waze, Google Assistant, and more. Upgrade to Music Premium (available in select countries) to enjoy: ● Listen to music ad-free ● Play music in the background ● Access your music downloads, including smart downloads ● Switch seamlessly between song audio and music videos, only with YouTube Music ---------- Only first-time YouTube Red, Music Premium, YouTube Premium and Google Play Music subscribers are eligible for free trials, introductory offers or promotional pricing.
