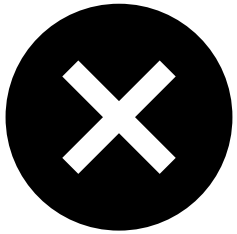
MOBSF

ANDROID STATIC ANALYSIS REPORT



Chrome (91.0.4472.114)

File Name:	Chrome.apk

Package Name:	com.android.chrome
Scan Date:	March 9, 2024, 9:57 a.m.
App Security Score:	48/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	44	1	1	1

FILE INFORMATION

File Name: Chrome.apk
Size: 23.9MB
MD5: 14d4580ce102e24535073ea1351d9992
SHA1: 051ea74cf963634944a5776757271ddcfbe23b2f
SHA256: c49dadd6babf21216e37bd03e74e14d44a8a4191b727914b220b3e49616b7cea

APP INFORMATION

App Name: Chrome
Package Name: com.android.chrome
Main Activity:
Target SDK: 30
Min SDK: 29
Max SDK:
Android Version Name: 91.0.4472.114
Android Version Code: 447211483

APP COMPONENTS

Activities: 54
Services: 78
Receivers: 32
Providers: 5
Exported Activities: 17
Exported Services: 8
Exported Receivers: 8

Exported Providers: 3

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2008-08-21 23:13:34+00:00
Valid To: 2036-01-07 23:13:34+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xc2e08746644a308d
Hash Algorithm: md5
md5: cde9f6208d672b54b1dacc0b7029f5eb
sha1: 38918a453d07199354f8b19af05ec6562ced5788
sha256: f0fd6c5b410f25cb25c3b53346c8972fae30f8ee7411df910480ad6b2d60db83
sha512: edf99db872937471eb94cbe576512a0089527e28b5b65df96f18f539737955ef1ce2553a51156ee31b521dcdc1559c52e965899f13038487d03743742b634326
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 843817f137559b510590075c0256a414a5767c6f32f91a46228077c065ba67fe
Found 1 unique certificates

APPLICATION PERMISSIONS

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.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_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.QUERY_ALL_PACKAGES	normal	enables querying any normal app on the device.	Allows query of any normal app on the device, regardless of manifest declarations.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_SYNC_SETTINGS	normal	read sync settings	Allows an application to read the sync settings, such as whether sync is enabled for Contacts.
android.permission.READ_SYNC_STATS	normal	read sync statistics	Allows an application to read the sync stats; e.g. the history of syncs that have occurred.
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
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.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WRITE_SYNC_SETTINGS	normal	write sync settings	Allows an application to modify the sync settings, such as whether sync is enabled for Contacts.
com.android.chrome.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.android.chrome.permission.READ_WRITE_BOOKMARK_FOLDERS	unknown	Unknown permission	Unknown permission from android reference
com.android.chrome.TOS_ACKED	unknown	Unknown permission	Unknown permission from android reference
com.chrome.permission.DEVICE_EXTRAS	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.android.launcher.permission.INSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
com.google.android.apps.now.CURRENT_ACCOUNT_ACCESS	unknown	Unknown permission	Unknown permission from android reference
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.sec.enterprise.knox.MDM_CONTENT_PROVIDER	unknown	Unknown permission	Unknown permission from android reference
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.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.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>assets/webapk7.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>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.BOARD check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes10.dex	FINDINGS / DETAILS yara_issue — yara issue - dex file recognized by apkid but not yara module Compiler — unknown (please file detection issue!)
classes11.dex	FINDINGS / DETAILS yara_issue — yara issue - dex file recognized by apkid but not yara module Anti-VM Code — Build.HARDWARE check Compiler — unknown (please file detection issue!)
classes2.dex	FINDINGS / DETAILS yara_issue — yara issue - dex file recognized by apkid but not yara module Anti-VM Code — Build.HARDWARE check Compiler — unknown (please file detection issue!)

FILE	DETAILS
classes3.dex	FINDINGS: yara_issue — DETAILS: yara issue - dex file recognized by apkid but not yara module FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)
classes4.dex	FINDINGS: yara_issue — DETAILS: yara issue - dex file recognized by apkid but not yara module FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)
classes5.dex	FINDINGS: yara_issue — DETAILS: yara issue - dex file recognized by apkid but not yara module FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)
classes6.dex	FINDINGS: yara_issue — DETAILS: yara issue - dex file recognized by apkid but not yara module FINDINGS: Anti-VM Code — DETAILS: Build.MANUFACTURER check Build.HARDWARE check FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes7.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes8.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes9.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.BOARD check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.google.android.apps.chrome.IntentDispatcher	Schemes: googlechrome://, http://, https://, about://, javascript://, content://, file://, Hosts: *, Mime Types: text/html, text/plain, application/xhtml+xml, multipart/related, message/rfc822, */*, Path Patterns: /.*.mhtml, /.*.mht, /.*..*.mhtml, /.*..*.mht, /.*..*..*.mhtml, /.*..*..*.mht, /.*..*..*..*.mhtml, /.*..*..*..*.mht, /.*..*..*..*..*.mhtml, /.*..*..*..*..*.mht, /.*..*..*..*..*..*.mhtml, /.*..*..*..*..*..*.mht, /.*..*..*..*..*..*..*.mhtml, /.*..*..*..*..*..*..*.mht, /.*..*..*..*..*..*..*..*.mhtml, /.*..*..*..*..*..*..*..*.mht, /.*..*..*..*..*..*..*..*..*.mhtml, /.*..*..*..*..*..*..*..*..*.mht,

NETWORK SECURITY

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

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

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm vulnerable to hash collision	high	Application is signed with MD5. MD5 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 0 | WARNING: 38 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App has a Network Security Configuration [android:networkSecurityConfig=@xml/APKTOOL_DUMMYVAL_0x7f170020]	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.
2	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.
3	Activity-Alias (com.google.android.apps.chrome.TranslateDispatcher) is Protected by a permission. Permission: com.android.chrome.permission.TRANSLATE protectionLevel: signature [android:exported=true]	info	An Activity-Alias is found to be exported, but is protected by permission.
4	Activity-Alias (com.google.android.apps.chrome.IntentDispatcher) 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.
5	Activity (org.chromium.chrome.browser.media.MediaLauncherActivity) 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-Alias (org.chromium.chrome.browser.media.AudioLauncherActivity) 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.
7	Activity (org.chromium.chrome.browser.incognito.IncognitoTabLauncher) 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.
8	Broadcast Receiver (org.chromium.chrome.browser.sharing.click_to_call.ClickToCallMessageHandler$PhoneUnlockedReceiver) 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
9	Activity (org.chromium.chrome.browser.ChromeTabbedActivity) 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.
10	Activity-Alias (com.google.android.apps.chrome.Main) 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	TaskAffinity is set for activity (org.chromium.chrome.browser.ChromeTabbedActivity2)	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.
12	Activity (org.chromium.chrome.browser.bookmarks.BookmarkAddActivity) 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 (org.chromium.chrome.browser.webapps.WebappLauncherActivity) 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.
14	Activity (org.chromium.chrome.browser.webapps.ActivateWebApkActivity) 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.
15	Activity (org.chromium.chrome.browser.printing.PrintShareActivity) 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.
16	Activity (org.chromium.chrome.browser.send_tab_to_self.SendTabToSelfShareActivity) 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
17	Activity (org.chromium.chrome.browser.sharing.shared_clipboard.SharedClipboardShareActivity) 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	Broadcast Receiver (org.chromium.chrome.browser.browserservices.ClientAppBroadcastReceiver) 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.
19	Activity (org.chromium.chrome.browser.browserservices.ManageTrustedWebActivityDataActivity) 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	Activity (org.chromium.chrome.browser.webauth.authenticator.CableAuthenticatorActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.cryptauth.permission.CABLEV2_SERVER_LINK [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.
21	Broadcast Receiver (org.chromium.chrome.browser.services.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.
22	Broadcast Receiver (com.google.android.apps.chrome.appwidget.bookmarks.BookmarkThumbnailWidgetProvider) 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.
23	Broadcast Receiver (org.chromium.chrome.browser.searchwidget.SearchWidgetProvider) 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
24	Service (com.google.ipc.invalidation.ticl.android2.channel.GcmRegistrationTaskService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_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.
25	Service (org.chromium.components.background_task_scheduler.internal.BackgroundTaskGcmTaskService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_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.
26	Service (org.chromium.chrome.browser.ChromeBackgroundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_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.
27	Service (org.chromium.chrome.browser.prerender.ChromePrerenderService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
28	Service (org.chromium.chrome.browser.customtabs.CustomTabsConnectionService) 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	Service (org.chromium.components.payments.PaymentDetailsUpdateService) 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.
30	Activity (org.chromium.chrome.browser.test_dummy.TestDummyActivity) 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.
31	Broadcast Receiver (com.google.android.apps.chrome.icing.AppIndexingUpdateReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.APPINDEXING [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.
32	Broadcast Receiver (com.google.android.apps.chrome.search_engines.SearchEngineChoiceNotificationReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.android.chrome.permission.SHOW_COMPLIANCE_SCREEN protectionLevel: signatureOrSystem [android:exported=true]	info	A Broadcast Receiver is found to be exported, but is protected by a permission. However, the protection level of the permission is set to signatureOrSystem. It is recommended that signature level is used instead. Signature level should suffice for most purposes, and does not depend on where the applications are installed on the device.
33	Broadcast Receiver (com.google.android.apps.chrome.webapps.WebApkInstallStatusReceiver) 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
34	Service (org.chromium.components.payments.GooglePayDataCallbacksService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_PAYMENTS_CALLBACK_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.
35	Service (org.chromium.chrome.browser.usage_stats.UsageStatsBrowserServiceProvider) 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.
36	Activity (org.chromium.chrome.browser.usage_stats.UsageStatsConsentActivity) 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.
37	Content Provider (org.chromium.chrome.browser.provider.ChromeBrowserProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
38	Content Provider (com.google.android.apps.chrome.autofill.AutofillDataProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
39	Content Provider (com.google.android.apps.chrome.icing.IcingProvider) is not Protected. [android:exported=true]	warning	A Content Provider 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
40	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.
41	Activity (com.google.android.libraries.surveys.internal.view.SurveyActivity) 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.

</> CODE ANALYSIS

HIGH: **0** | WARNING: **5** | INFO: **1** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/A12.java defpackage/AD1.java defpackage/AbstractBinderC3406a41.java defpackage/AbstractC0993Hq2.java defpackage/AbstractC11516yd4.java defpackage/AbstractC11780zR1.java defpackage/AbstractC11858zf4.java defpackage/AbstractC2165Qr0.java defpackage/AbstractC2415Sp0.java defpackage/AbstractC2545Tp0.java defpackage/AbstractC3224Yv.java defpackage/AbstractC3449aB3.java defpackage/AbstractC4008bt1.java defpackage/AbstractC4702e.java defpackage/AbstractC5235fb4.java defpackage/AbstractC6379i40.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/AbstractC6397j70.java defpackage/AbstractC7382m61.java defpackage/AbstractC7813nP3.java defpackage/AbstractC8168oU3.java defpackage/AbstractC8241oh4.java defpackage/AbstractC8984qy0.java defpackage/AbstractC9112rL3.java defpackage/AbstractDialogInterface$OnClickListenerC7954nq0.java defpackage/C10204uf0.java defpackage/C10489vX0.java defpackage/C10790wR1.java defpackage/C11120xR1.java defpackage/C11810zX1.java defpackage/C11892zm.java defpackage/C11898zn0.java defpackage/C1685Mz0.java defpackage/C2629Ug.java defpackage/C2660Um0.java defpackage/C3008Xd3.java defpackage/C3152Yg2.java defpackage/C4131cF3.java defpackage/C4505dO1.java defpackage/C6488jO3.java defpackage/C6790kJ0.java defpackage/C7015l00.java defpackage/C7024l13.java defpackage/C8.java defpackage/C8042o61.java defpackage/C8243oi0.java defpackage/C9176rY2.java defpackage/C9727tC3.java defpackage/C9890th4.java defpackage/CA3.java defpackage/CB3.java defpackage/D21.java defpackage/ED1.java defpackage/EX0.java defpackage/FR1.java defpackage/G93.java defpackage/GD1.java defpackage/GW1.java defpackage/H34.java defpackage/H61.java defpackage/HD1.java defpackage/I34.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/IN1.java defpackage/LD1.java defpackage/NC1.java defpackage/NR1.java defpackage/OC1.java defpackage/OI3.java defpackage/OR1.java defpackage/P4.java defpackage/PC1.java defpackage/RunnableC10292uw.java defpackage/RunnableC7840nV0.java defpackage/SN.java defpackage/VI2.java defpackage/ViewTreeObserver$OnPreDrawListenerC7913ni0.java defpackage/Y01.java
2	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	defpackage/NH0.java defpackage/ZJ.java
3	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/AbstractC4173cO0.java defpackage/AbstractC6397j70.java
4	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	defpackage/C11446yQ2.java defpackage/C8139oP.java
5	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/AK.java
6	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/C9176rY2.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libmonochrome_stack_unwinder_partition.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	armeabi-v7a/libmonochrome_test_dummy_partition.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
3	armeabi-v7a/libmonochrome_vr_partition.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
4	armeabi-v7a/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
5	armeabi-v7a/libsketchology_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', '__strchr_chk', '__memcpy_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	armeabi-v7a/libarcore_sdk_c.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	armeabi-v7a/libmonochrome_cablev2_authenticator_partition.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	armeabi-v7a/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: ['__strchr_chk', '__memcpy_chk', '__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	armeabi-v7a/libchromium_android_linker.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: ['__strlcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	armeabi-v7a/libmonochrome_stack_unwinder_partition.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
11	armeabi-v7a/libmonochrome_test_dummy_partition.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
12	armeabi-v7a/libmonochrome_vr_partition.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	armeabi-v7a/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
14	armeabi-v7a/libsketchology_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', '__strchr_chk', '__memcpy_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	armeabi-v7a/libarcore_sdk_c.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	armeabi-v7a/libmonochrome_cablev2_authenticator_partition.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
17	armeabi-v7a/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: ['__strchr_chk', '__memcpy_chk', '__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	armeabi-v7a/libchromium_android_linker.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: ['__strlcpy_chk']	False warning Symbols are available.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	14/24	android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.GET_ACCOUNTS, android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.RECORD_AUDIO, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_WIFI_STATE, android.permission.READ_CONTACTS
Other Common Permissions	8/45	android.permission.CHANGE_NETWORK_STATE, android.permission.FOREGROUND_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.c2dm.permission.RECEIVE, com.android.launcher.permission.INSTALL_SHORTCUT, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.REQUEST_INSTALL_PACKAGES

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.eksempel.dk	ok	**IP:** 193.163.102.59 **Country:** Sweden **Region:** Stockholms lan **City:** Stockholm **Latitude:** 59.332581 **Longitude:** 18.064899 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
schemas.android.com	ok	No Geolocation information available.
google.com	ok	**IP:** 142.251.10.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
dev-notifications-pa.corp.googleapis.com	ok	**IP:** 74.125.68.129 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
families.google.com	ok	**IP:** 142.251.10.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
chromestatus.com	ok	**IP:** 216.239.32.21 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
lh3.googleusercontent.com	ok	**IP:** 74.125.200.132 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
plus.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
cloud.google.com	ok	**IP:** 74.125.130.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
memex-pa.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
autopush-proddata-notifications-pa.sandbox.googleapis.com	ok	**IP:** 142.251.175.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
bit.ly	ok	**IP:** 67.199.248.10 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
developers.google.com	ok	**IP:** 74.125.24.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.gov.uk	ok	**IP:** 199.232.44.144 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
play.google.com	ok	**IP:** 142.251.10.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
www.chromestatus.com	ok	**IP:** 74.125.130.121 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 142.251.175.99 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.primer.si	ok	**IP:** 151.101.192.119 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
developer.android.com	ok	**IP:** 172.253.118.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.ejemplo.com	ok	**IP:** 199.59.243.225 **Country:** United States of America **Region:** Florida **City:** Tampa **Latitude:** 27.943518 **Longitude:** -82.510269 **View:** Google Map
www.chromium.org	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
notifications-pa.googleapis.com	ok	**IP:** 74.125.200.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
autopush-notifications-pa.sandbox.googleapis.com	ok	**IP:** 142.251.175.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gl	ok	**IP:** 142.251.10.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
myaccount.google.com	ok	**IP:** 74.125.130.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
staging-notifications-pa.sandbox.googleapis.com	ok	**IP:** 64.233.170.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
symbolize.corp.google.com	ok	**IP:** 142.251.12.129 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
foo.example.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
policies.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
support.google.com	ok	**IP:** 142.251.175.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
308203c7308202afa003020102021500dc286b43b4ea12039958a00a6655eb84720e46c9300d06092a864886f70d01010b05003074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f6964311030 00e060355040313307416e64726f6964301e170d3137303830343136353333375a170d3437303830343136353333375a3074310b3009060355040613025553311330110603550408130a43616c 69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e0603 5504031307416e64726f696430820122300d06092a864886f70d01010105000382010f003082010a0282010100898646f47fc333db09644c303104ed183e904e351152aa66a603b77f63389d45 d6fcffae3c94fadf1f28038e265d697fea347327f9081a7f0b9074d5b148db5bf357c611a77f87f844a15068818bdcd5b21d187e93fa2551676170eedce04a150c35ec0a791eef507fa9b406573c36f 6f207764842e5677e35a281a422659e91e26eb4fecfb053b5c936d0976c37f8757adb57a37953da5844ea350695854d343a61ad341b63a1c425d22855af7ebfee018e1736cee98536be5b9947f2 88e2a26f99eb9f91b5de93fecc513019d2e90f12b38610d1f02eaa81deca4ce91c19cbce36d6c3025ce2432b3d178616beafaf437c08451bc469c6bc6f4517a714a5b0203010001a350304e300c06 03551d13040530030101ff301d0603551d0e0416041419a864c0f2618c67c803a23da909bc70521f269b301f0603551d230418301680141 9a864c0f2618c67c803a23da909bc70521f269b300d06092a864886f70d01010b05000382010100 5403fc56fdefc440376a0337815002b96a15bffc2fe42de6c58f52fae4d80652e3704455b885409eef81ffbb4c44dba104b6b8e24c9e2e0e7a04338ee73baa5b71bfb4488f8e04bef3d0eaf7d43aa42b03b278c33cc1f0dd3802571624baa161d851fab37db4bc92b9094b6885dff62b400ecd81f069d56a1be1db46d8198c50c9628cdb6e38686ef640fd3 86775f50376f957e24ea45ed1942968f20c82f189607fdb22f11cfdfd0760a77a60ceb3416cfb3f48f13f9f83f3834a01001750a7c78bc1fd81f0b53a7c41dcba9f5a0118259d083c32bb9ebb84d645 d6f6b9c31923d8ab70e7f0a25940ecc9f4945144419f86e8c421d3b99774f4b8f3d09262e7

PLAYSTORE INFORMATION

Title: Google Chrome: Fast & Secure

Score: 4.062299 **Installs:** 10,000,000,000+ **Price:** 0 **Android Version Support:** **Category:** Communication **Play Store URL:** com.android.chrome

Developer Details: Google LLC, 5700313618786177705, 1600 Amphitheatre Parkway, Mountain View 94043, http://www.google.com/chrome/android, apps-help@google.com,

Release Date: Feb 7, 2012 **Privacy Policy:** Privacy link

Description:

Google Chrome is a fast, easy to use, and secure web browser. Designed for Android, Chrome brings you personalized news articles, quick links to your favorite sites, downloads, and Google Search and Google Translate built-in. Download now to enjoy the same Chrome web browser experience you love across all your devices. Browse fast and type less. Choose from personalized search results that instantly appear as you type and quickly browse previously visited web pages. Fill in forms quickly with Autofill. Incognito Browsing. Use Incognito mode to browse the internet without saving your history. Browse privately across all your devices. Access your Chrome across devices. When you sign in to Chrome, you can save bookmarks, passwords and more in your Google Account, so you can access them on your other devices. All your favorite content, one tap away. Chrome is not just fast for Google Search, but designed so you are one tap away from all your favorite content. You can tap on your favorite news sites or social media directly from the new tab page. Chrome also has the “Tap to Search”- feature on most webpages. You can tap on any word or phrase to start a Google search while still in the page you are enjoying. Protect your phone with Google Safe Browsing. Chrome has Google Safe Browsing built-in. It keeps your phone safe by showing warnings to you when you attempt to navigate to dangerous sites or download dangerous files. Fast downloads and view web pages and videos offline Chrome has a dedicated download button, so you can easily download videos, pictures, and entire webpages with just one tap. Chrome also has downloads home right inside Chrome, where you can access all the content you downloaded, even when you are offline. Google Voice Search. Chrome gives you an actual web browser you can talk to. Use your voice to find answers on-the-go without typing and go hands free. You can browse and navigate quicker using your voice anywhere, anytime. Google Translate built-in: Quickly translate entire web pages. Chrome has Google Translate built in to help you to translate entire web to your own language with one tap. Smart personalized recommendations. Chrome creates an experience that is tailored to your interests. On the new tab page, you will find articles that Chrome selected based on your previous browsing history.

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.