MOBSF

ANDROID STATIC ANALYSIS REPORT

Parental Control Kroha (3.10.4)

File Name:	Parental Control Kroha_merged.apk
Package Name:	ua.com.tim_berners.parental_control
Scan Date:	Aug. 11, 2024, 4:20 p.m.

App Security Score: 51/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	23	2	2	1

FILE INFORMATION

File Name: Parental Control Kroha_merged.apk
Size: 16.0MB

MD5: eb38efc63f453d053df9c03b3a72920f
SHA1: b241c26cd8aa0c9f9aea23f426d4fac513525612
SHA256: 87bc0a6597ec50e3f66d1df1fc1249bb8003b5e26dd0919ace76a0f86c2cbe99

APP INFORMATION

App Name: Parental Control Kroha
Package Name: ua.com.tim_berners.parental_control
Main Activity: ua.com.tim_berners.parental_control.ui.main.SplashActivity
Target SDK: 33
Min SDK: 21
Max SDK:
Android Version Name: 3.10.4
Android Version Code: 770

APP COMPONENTS

Activities: 23
Services: 31
Receivers: 15
Providers: 3
Exported Activities: 5
Exported Services: 4
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: False
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: 2018-05-04 23:22:23+00:00
Valid To: 2048-05-04 23:22:23+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xd493b73097d2d501438c8809014af67c77e605f7
Hash Algorithm: sha256
md5: 17ab6742740ca271937b6dfe7b920ad0
sha1: 963df8ea187726188cdf1fe179ec81553c4a41b9
sha256: 45df3b0b988b0f7724730c0759f9ff33a23257c35550f9837b59dbd6b210cdef
sha512: 18b1341cc107ee5c8a42e596e1f2c4634e0f9d4ad314e13c2fa849c97f803ee2106080d00ffee13106f3dc14bc3899c1beaf2e962f3212b2b895b891f86ebc55
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 317c58e0e82e78b7d48251cf6c3da9384249a90ba813f75d142b198ac20d4d64
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.BROADCAST_CLOSE_SYSTEM_DIALOGS	unknown	Unknown permission	Unknown permission from android reference
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.READ_PRIVILEGED_PHONE_STATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.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.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
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.BIND_ACCESSIBILITY_SERVICE	signature	required by AccessibilityServices for system binding.	Must be required by an AccessibilityService, to ensure that only the system can bind to it.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.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.
oppo.permission.OPPO_COMPONENT_SAFE	signature	permission specific to OPPO devices	It is used to grant apps the ability to access certain system-level features or components that are otherwise restricted for security reasons. This permission ensures that only trusted applications can interact with sensitive parts of the OPPO system.
com.huawei.permission.external_app_settings.USE_COMPONENT	signature	permission specific to Huawei devices	It is used to grant apps the ability to access certain system-level features or components that are otherwise restricted for security reasons. This permission ensures that only trusted applications can interact with sensitive parts of the Huawei system.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
ua.com.tim_berners.parental_control.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator check
network operator name check
ro.hardware check
ro.kernel.qemu check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.BOARD check
possible Build.SERIAL check
subscriber ID check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
ua.com.tim_berners.parental_control.ui.main.MainActivity	Schemes: parentalcontrolkroha://,
ua.com.tim_berners.parental_control.ui.main.BlockedActivity	Schemes: parentalcontrolkroha://,
ua.com.tim_berners.parental_control.ui.main.SplashActivity	Schemes: parentalcontrolkroha://,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

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

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

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **13** | 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	Activity (ua.com.tim_berners.parental_control.ui.auth.LoginActivity) 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.
3	Activity (ua.com.tim_berners.parental_control.ui.auth.AutoLoginActivity) 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.
4	Activity (ua.com.tim_berners.parental_control.ui.main.MainActivity) 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
5	Activity (ua.com.tim_berners.parental_control.ui.main.BlockedActivity) 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 (ua.com.tim_berners.parental_control.ui.main.EyeProtectionBlockActivity) 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.
7	Service (ua.com.tim_berners.parental_control.service.DeviceOwnerService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_DEVICE_ADMIN [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.
8	Service (ua.com.tim_berners.parental_control.service.vpn.netguard.ServiceSinkhole) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_VPN_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.
9	Broadcast Receiver (ua.com.tim_berners.parental_control.service.ConnectReceiver) 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.
10	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.
11	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.
12	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) 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.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
14	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 8 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a1/d.java a6/g.java a8/b.java ag/p.java b1/a.java b2/c.java b2/e.java b8/c.java butterknife/ButterKnife.java c2/h.java c2/i.java c2/k.java c2/q.java c2/z.java c4/b.java c7/g.java com/appsflyer/api/PurchaseClient.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1qSDK.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1jSDK.java com/appsflyer/internal/AFf1kSDK.java com/appsflyer/internal/AFg1jSDK.java com/bumptech/glide/b.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java com/bumptech/glide/manager/e.java com/bumptech/glide/manager/p.java com/bumptech/glide/manager/q.java com/miui/referrer/commons/LogUtils.java d2/i.java d2/k.java d4/g.java d4/p.java d4/q.java d5/a.java dc/b.java dc/d.java df/c7.java df/i1.java df/p.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	e1/b.java e1/e.java e2/i.java e3/k.java f1/m0.java f2/a.java f5/a.java f5/d.java f7/r.java g2/c.java g2/d.java g2/g.java g2/t.java g2/u.java g2/v.java g4/h.java g5/c.java h1/i.java h3/a.java h4/d.java h5/a.java i2/l.java io/github/dreierf/materialintroscreen/widgets/CustomViewPager.java io/github/inflationx/calligraphy3/ReflectionUtils.java io/github/inflationx/calligraphy3/TypefaceUtils.java io/realm/internal/OsRealmConfig.java io/realm/internal/f.java io/realm/mongodb/sync/Sync.java io/realm/mongodb/sync/SyncSession.java j2/a0.java j2/c.java j2/f.java j2/j0.java j2/m0.java j2/o.java j2/v.java j2/w.java j4/b.java j4/d.java j4/f.java j4/h.java j5/h.java j8/d0.java j8/g0.java j8/h.java j8/j0.java j8/l.java j8/y.java k0/a.java k8/a.java l6/f.java l8/c.java l8/f.java m/d.java n2/a.java n2/d.java n2/j.java o9/m.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o9/u.java p0/a.java p2/d.java q3/a.java q3/d.java r/a.java r2/i.java s2/i.java t0/d.java t9/c.java u3/a.java u3/d.java u3/l.java u3/n.java u3/p.java u3/s.java u3/t.java u8/d.java ua/com/tim_berners/parental_control/billing/BillingManager.java ua/com/tim_berners/parental_control/service/eye_protection/CameraSourcePreview.java ua/com/tim_berners/parental_control/service/vpn/netguard/ServiceSinkhole.java ua/com/tim_berners/parental_control/ui/category/contacts/ContactsFragment.java v0/o.java v0/r.java v0/u.java v0/y.java v3/n.java v4/d.java w/f.java w2/a.java w3/m0.java w4/n.java w6/f.java w8/e.java x0/a.java x5/d.java y/c.java y1/d.java y1/e.java y5/b.java z0/h.java z1/a.java z3/d0.java z3/h0.java z3/q.java z3/t.java z3/v.java z6/g.java z6/o.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/appsflyer/internal/AFb1hSDK.java com/appsflyer/internal/AFc1fSDK.java com/appsflyer/internal/connector/purcahse/AFPurchaseConnectorA1y.java ob/a.java ua/com/tim_berners/parental_control/ui/category/sounds/ListenVoiceFragment.java
3	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	a2/h.java c2/d.java c2/p.java c2/x.java g7/b.java h7/e.java h7/w.java m1/d.java ua/com/tim_berners/parental_control/service/app_block/BlockSettingsHelper.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	io/realm/mongodb/sync/Sync.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	a8/b.java ua/com/tim_berners/parental_control/billing/Security.java v8/o.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	bf/a.java df/g3.java ua/com/tim_berners/parental_control/service/vpn/netguard/ServiceSinkhole.java
7	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	f7/i.java l6/w.java
8	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	a1/c.java l3/m0.java l3/t0.java t8/e.java
9	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	ag/m0.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	ag/y0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/appsflyer/internal/AFb1vSDK.java
12	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	a8/c.java v0/y.java
13	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	ua/com/tim_berners/parental_control/ui/category/contacts/ContactsFragment.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	x86_64/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__vsnprintf_chk', '__strchr_chk', '__vsprintf_chk', '__read_chk', '__FD_SET_chk']	False warning Symbols are available.
2	x86_64/libnetguard.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: ['__strcpy_chk', '__vsprintf_chk', '__strlen_chk', '__memcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	x86_64/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__vsnprintf_chk', '__strchr_chk', '__vsprintf_chk', '__read_chk', '__FD_SET_chk']	False warning Symbols are available.
4	x86_64/libnetguard.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: ['__strcpy_chk', '__vsprintf_chk', '__strlen_chk', '__memcpy_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_WIFI_STATE, android.permission.READ_CONTACTS, android.permission.READ_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.CAMERA, android.permission.WAKE_LOCK, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.SYSTEM_ALERT_WINDOW, android.permission.VIBRATE, android.permission.READ_PHONE_STATE, android.permission.RECORD_AUDIO
Other Common Permissions	9/45	android.permission.WRITE_CONTACTS, com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, android.permission.ACCESS_NOTIFICATION_POLICY, android.permission.ACCESS_BACKGROUND_LOCATION, com.google.android.gms.permission.AD_ID, android.permission.PACKAGE_USAGE_STATS, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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

Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
sattr.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
docs.mongodb.com	ok	**IP:** 151.101.2.133 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.facebook.com	ok	**IP:** 31.13.84.36 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.
www.google.com	ok	**IP:** 142.250.180.228 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
advanced.parental-control.net	ok	**IP:** 116.203.4.110 **Country:** Germany **Region:** Bayern **City:** Gunzenhausen **Latitude:** 48.323330 **Longitude:** 11.601220 **View:** Google Map
firebase.google.com	ok	**IP:** 142.251.39.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.251.208.130 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sapp.s	ok	No Geolocation information available.
api.parentalcontrolkroha.net	ok	**IP:** 116.203.4.110 **Country:** Germany **Region:** Bayern **City:** Gunzenhausen **Latitude:** 48.323330 **Longitude:** 11.601220 **View:** Google Map
scdn-ssettings.s	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.
scdn-stestsettings.s	ok	No Geolocation information available.
www.youtube.com	ok	**IP:** 172.217.19.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sconversions.s	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.
issuetracker.google.com	ok	**IP:** 142.250.201.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 142.250.180.227 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
smonitorsdk.s	ok	No Geolocation information available.
realm.mongodb.com	ok	**IP:** 3.127.11.207 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
api.mixpanel.com	ok	**IP:** 107.178.240.159 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
twitter.com	ok	**IP:** 104.244.42.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
sviap.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
svalidate.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.
youtu.be	ok	**IP:** 142.251.208.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ssdk-services.s	ok	No Geolocation information available.
play.google.com	ok	**IP:** 142.251.208.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sars.s	ok	No Geolocation information available.
m.youtube.com	ok	**IP:** 142.250.180.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
simpression.s	ok	No Geolocation information available.
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
parental-control-5086b.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
parental-control.net	ok	**IP:** 116.203.4.110 **Country:** Germany **Region:** Bayern **City:** Gunzenhausen **Latitude:** 48.323330 **Longitude:** 11.601220 **View:** Google Map
developer.android.com	ok	**IP:** 142.251.39.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sinapps.s	ok	No Geolocation information available.

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://parental-control-5086b.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
support@parental-control.net	ua/com/tim_berners/parental_control/ui/sidemenu/SupportFragment.java
support@parental-control.net	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"google_maps_key" : "AIzaSyAIfAsXmk0gJltyLTA67toOy5-z2ENt12s"
"google_crash_reporting_api_key" : "AIzaSyBtK4wTdA1smHXj5DwYZEqxTiJ0BO_rFIM"
"firebase_database_url" : "https://parental-control-5086b.firebaseio.com"
"com.google.firebase.crashlytics.mapping_file_id" : "5d20e184c945455b8b8067d5de9badd9"
"google_api_key" : "AIzaSyBtK4wTdA1smHXj5DwYZEqxTiJ0BO_rFIM"
8c062dcbf247e7db5cf74ca013d77a32
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
470fa2b4ae81cd56ecbcda9735803434cec591fa
85053bf24bba75239b16a601d9387e17
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
5181942b9ebc31ce68dacb56c16fd79f
ae2044fb577e65ee8bb576ca48a2f06e
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1

PLAYSTORE INFORMATION

Title: Parental Control Kroha

Score: 3.7 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Parenting **Play Store URL:** ua.com.tim_berners.parental_control

Developer Details: Parental Control Kroha, Parental+Control+Kroha, Kyiv, Pushkinska str. 10, https://parental-control.net, support@parental-control.net,

Release Date: May 12, 2018 **Privacy Policy:** Privacy link

Description:

The parental control app for android is created to protect kids and provides supervision to keep kids safe online. The app is a powerful child control app for screen time, tracking location, tracking application usage time, limit app usage, limit phone usage, website control, YouTube monitoring. You can block apps, set daily app time limit, limit screen time, block inappropriate content. The application has unique features such as monitoring social media chats and eyes protection. Use night mode and eyes protection features to form healthy habits for your kids' eyes. ★ App lock & Phone lock: • Block apps and block games • Block social media apps • Limit app usage time and limit usage time remotely • Set schedules and limit phone usage for family time, bedtime and study time ★ Device screen time management: • Screen time app shows a detailed view of the daily phone usage • Set and manage a specific daily app time limit • Screen time tracker allows you to monitor apps usage statistics ★ Social media chat monitoring: • Monitoring messengers (WhatsApp, Viber) • YouTube Monitoring ★ Eyes protection & Night mode: • Use Night Mode to protect the child's eyes from intense blue light in the evening • Use eyes protection to keep your child's phone screen at the correct distance from your eyes ★ Family Locator & GPS tracking: • Monitor your child's location on the map in real-time • Set geo-zone and get notifications if a child leaves this zone ★ Block websites & Block Youtube videos: • Monitor websites which your child visited • Web filters allow you to safe kids from harmful sites and content • Monitor YouTube videos which your child was watched • Block YouTube videos and channels • Turn on Safe Search function to protect your kid's searches online also app gives you an opportunity to: • Monitor and manage your kid's phonebook • Monitor the latest kid's photos • Monitor the battery level of the kids' phone Use "Parental Control apps Kroha - Screen time & Kids Mode" to improve your family links. Spend more family time without mobile phones. Please install this application on your mobile smartphone and then on your child's one(s) to perform remote child control of a child's device. Link all your family devices to the account. Both smartphones should have network data capability, as the app uses data to send and receive configuration commands. The application is designed exclusively for children's protection and child safety. If the application is used inappropriately, the company disclaims responsibility for the consequences. Price for the one-year license includes controlling of five different family devices, which can be activated in any mode (Parent mode / Kids mode). Use one account for the whole family. Check out the subscription price: https://parental-control.net Feedback If you have any issues or questions, you can always contact our support team: support@parental-control.net Troubleshooting notes: For all parental control apps and screen time apps users should set up Battery Saving Settings on your child's phone. Permissions • This app requires the VPN permission to block and filter inappropriate websites. • This app uses the Device Administrator permission • This app requires the Accessibility Service permission to save browsing history, website visits, and YouTube browsing history, as well as instant messengers history, which allows provide you with reports on your child's device usage. The Accessibility Service permission is also used to detect attempts to uninstall the app.

SCAN LOGS

Timestamp	Event	Error
2024-08-11 16:20:43	Generating Hashes	OK
2024-08-11 16:20:43	Extracting APK	OK
2024-08-11 16:20:43	Unzipping	OK
2024-08-11 16:20:46	Getting Hardcoded Certificates/Keystores	OK
2024-08-11 16:21:00	Parsing AndroidManifest.xml	OK
2024-08-11 16:21:00	Parsing APK with androguard	OK

2024-08-11 16:21:02	Extracting Manifest Data	OK
2024-08-11 16:21:02	Performing Static Analysis on: Parental Control Kroha (ua.com.tim_berners.parental_control)	OK
2024-08-11 16:21:02	Fetching Details from Play Store: ua.com.tim_berners.parental_control	OK
2024-08-11 16:21:04	Manifest Analysis Started	OK
2024-08-11 16:21:04	Checking for Malware Permissions	OK
2024-08-11 16:21:04	Fetching icon path	OK
2024-08-11 16:21:04	Library Binary Analysis Started	OK
2024-08-11 16:21:04	Analyzing lib/x86_64/librealm-jni.so	OK
2024-08-11 16:21:16	Analyzing lib/x86_64/libnetguard.so	OK
2024-08-11 16:21:16	Analyzing apktool_out/lib/x86_64/librealm-jni.so	OK
2024-08-11 16:21:27	Analyzing apktool_out/lib/x86_64/libnetguard.so	OK
2024-08-11 16:21:28	Reading Code Signing Certificate	OK
2024-08-11 16:21:28	Failed to get signature versions	CalledProcessError(1, ['/jdk-20.0.2/bin/java', '-Xmx1024M', '-Djava.library.path=', '-jar', '/home/mobsf/Mobile-Security-Framework-MobSF/mobsf/StaticAnalyzer/tools/apksigner.jar', 'verify', '--verbose', '/home/mobsf/.MobSF/uploads/eb38efc63f453d053df9c03b3a72920f/eb38efc63f453d053df9c03b3a72920f.apk'])
2024-08-11 16:21:28	Running APKiD 2.1.5	OK
2024-08-11 16:21:33	Detecting Trackers	OK

2024-08-11 16:21:37	Decompiling APK to Java with jadx	OK
2024-08-11 16:24:08	Converting DEX to Smali	OK
2024-08-11 16:24:08	Code Analysis Started on - java_source	OK
2024-08-11 16:26:35	Android SAST Completed	OK
2024-08-11 16:26:35	Android API Analysis Started	OK
2024-08-11 16:27:59	Android Permission Mapping Started	OK
2024-08-11 16:29:52	Android Permission Mapping Completed	OK
2024-08-11 16:30:01	Finished Code Analysis, Email and URL Extraction	OK
2024-08-11 16:30:01	Extracting String data from APK	OK
2024-08-11 16:30:01	Extracting String data from SO	OK
2024-08-11 16:30:02	Extracting String data from Code	OK
2024-08-11 16:30:02	Extracting String values and entropies from Code	OK
2024-08-11 16:30:09	Performing Malware check on extracted domains	OK
2024-08-11 16:30:20	Saving to Database	OK