ANDROID STATIC ANALYSIS REPORT

Parental Time Control (1.5.108)

File Name:	ParentalControl_1.5.108.apk
Package Name:	com.rockman.dev
Scan Date:	Aug. 10, 2024, 6:56 p.m.

App Security Score: 48/100 (MEDIUM RISK)

Grade: B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
2	12	1	1	1

FILE INFORMATION

File Name: ParentalControl_1.5.108.apk

Size: 1.3MB

MD5: a0b4805bda024fa29f7f1e6c9338659e

SHA1: 74b0e541c3891b1bd234b9966efa54adf9087ccd

SHA256: 70fb543867604455402d0c0674e0b0031844a6daa295ea9ffeaf7587d41a4011

APP INFORMATION

App Name: Parental Time Control

Package Name: com.rockman.dev

Main Activity: com.rockman.dev.MainParentCtrl

Target SDK: 23

Min SDK: 23

Max SDK:

Android Version Name: 1.5.108

Android Version Code: 108

APP COMPONENTS

Activities: 18

Services: 10

Receivers: 4

Providers: 3

Exported Activities: 0

Exported Services: 4

Exported Receivers: 4

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed

v1 signature: True

v2 signature: True

v3 signature: False

v4 signature: False

X.509 Subject: C=373, ST=Chisinau, L=Chisinau, O=TeslineService SRL, OU=App Division, CN=Yurii Syrku

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2015-10-07 17:48:36+00:00

Valid To: 2045-09-29 17:48:36+00:00

Issuer: C=373, ST=Chisinau, L=Chisinau, O=TeslineService SRL, OU=App Division, CN=Yurii Syrku

Serial Number: 0x56155af4

Hash Algorithm: sha1

md5: 60f155902c4f4c11a5c98f01770c7e64

sha1: 3a954e689a38f2ae621c285471296b1c884c441b

sha256: 1bd83efa8aaf220460427f528857e36ef5c4bf20fc32c19f2231ba8f8a02ad98

sha512: aad4ba1f8f74d0196fb07b48d23b3ae61e3ba3e0656840201f91e5b30fca9ca305958f50e1ab5a1e22a61640fbef8277add6c8c7be757566b57bb4190e94c8e5
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 0e607b499c5bfd768ce26fc6775ba87c3b7092f86d2bb59684b36093ef3e37e5
Found 1 unique certificates

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
com.android.browser.permission.READ_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
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.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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.READ_CALL_LOG	dangerous	grants read access to the user's call log.	Allows an application to read the user's call log.
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.
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.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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check network operator name check</td></tr><tr><td>Compiler</td><td>r8</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

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

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

MANIFEST ANALYSIS

HIGH: **2** | WARNING: **8** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 6.0-6.0.1, [minSdk=23]	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	Broadcast Receiver (com.rockman.dev.OnBootReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
3	Broadcast Receiver (com.rockman.dev.AlarmReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
4	Service (com.rockman.dev.EmptyService) 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.
5	Broadcast Receiver (com.rockman.dev.parentctrl.DeviceAdminPCReceiver) 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 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.
6	Broadcast Receiver (com.rockman.dev.SmsReceiver) 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.
7	Activity (com.rockman.dev.parentctrl.AppMessages) is vulnerable to Android Task Hijacking/StrandHogg.	high	An Activity should not be having the launch mode attribute set to "singleTask". It is then possible for other applications to place a malicious activity on top of the activity stack resulting in Task Hijacking/StrandHogg 1.0 vulnerability. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" or by setting an empty taskAffinity (taskAffinity="") attribute. You can also update the target SDK version (23) of the app to 28 or higher to fix this issue at platform level.
8	Service (com.rockman.dev.parentctrl.services.PCJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
9	Service (com.rockman.dev.parentctrl.services.SLJobService) 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.
10	Service (com.rockman.dev.parentctrl.services.ForegroundService) 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.

CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	com/rockman/dev/parentctrl/contentprovider/AppDbHelper.java com/rockman/dev/parentctrl/contentprovider/AppSessionDbHelper.java
2	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	com/rockman/dev/AudioFilesList.java com/rockman/dev/MainParentCtrl.java com/rockman/dev/PCService.java com/rockman/dev/parentctrl/SetupWizard.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	com/rockman/dev/CallsReceiver.java com/rockman/dev/HelpActivity.java com/rockman/dev/MainParentCtrl.java com/rockman/dev/MultipartForm.java com/rockman/dev/Settings.java com/rockman/dev/ShowSysLogs.java com/rockman/dev/SysLog.java com/rockman/dev/TApplication.java com/rockman/dev/Templates.java com/rockman/dev/parentctrl/AppListAdapter.java com/rockman/dev/parentctrl/AppMessages.java com/rockman/dev/parentctrl/AppTimeList.java com/rockman/dev/parentctrl/AppsListAdapter.java com/rockman/dev/parentctrl/AppsTotalList.java com/rockman/dev/parentctrl/AuthenticationActivity.java com/rockman/dev/parentctrl/DataCollector.java com/rockman/dev/parentctrl/NotifyActivity.java com/rockman/dev/parentctrl/PCtrlSettings.java com/rockman/dev/parentctrl/SRService.java com/rockman/dev/parentctrl/SetupWizard.java com/rockman/dev/parentctrl/SysInfoBox.java com/rockman/dev/parentctrl/TimeChecker.java com/rockman/dev/parentctrl/TimePickerFragment.java com/rockman/dev/parentctrl/TimePickerPC.java com/rockman/dev/parentctrl/TimePickerPreference.java com/rockman/dev/parentctrl/contentprovider/AppDbHelper.java com/rockman/dev/parentctrl/contentprovider/AppProvider.java com/rockman/dev/parentctrl/contentprovider/AppSessionProvider.java com/rockman/dev/parentctrl/services/GetPreviousSms.java com/rockman/dev/parentctrl/services/PCJobService.java com/rockman/dev/parentctrl/services/SLJobService.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	17/24	android.permission.ACCESS_FINE_LOCATION, android.permission.INTERNET, android.permission.RECEIVE_SMS, android.permission.READ_SMS, android.permission.SEND_SMS, android.permission.READ_CONTACTS, android.permission.ACCESS_WIFI_STATE, android.permission.GET_TASKS, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_COARSE_LOCATION, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_CALL_LOG, android.permission.SYSTEM_ALERT_WINDOW, android.permission.READ_PHONE_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WAKE_LOCK
Other Common Permissions	4/45	android.permission.CHANGE_WIFI_STATE, android.permission.PACKAGE_USAGE_STATS, android.permission.FOREGROUND_SERVICE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

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
data.staffcounter.net	ok	**IP:** 95.217.199.78 **Country:** Finland **Region:** Uusimaa **City:** Helsinki **Latitude:** 60.169521 **Longitude:** 24.935450 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
kidlogger.net	ok	**IP:** 95.217.199.78 **Country:** Finland **Region:** Uusimaa **City:** Helsinki **Latitude:** 60.169521 **Longitude:** 24.935450 **View:** Google Map
market.android.com	ok	**IP:** 172.217.20.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schema.org	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
www.kidlogger.net	ok	**IP:** 95.217.199.78 **Country:** Finland **Region:** Uusimaa **City:** Helsinki **Latitude:** 60.169521 **Longitude:** 24.935450 **View:** Google Map

✉ EMAILS

EMAIL	FILE
help@kidlogger.net	com/rockman/dev/ShowLogs.java
help@kidlogger.net	com/rockman/dev/ShowSysLogs.java

☰ SCAN LOGS

Timestamp	Event	Error
2024-08-10 18:56:05	Generating Hashes	OK
2024-08-10 18:56:05	Extracting APK	OK
2024-08-10 18:56:05	Unzipping	OK
2024-08-10 18:56:05	Getting Hardcoded Certificates/Keystores	OK
2024-08-10 18:56:06	Parsing AndroidManifest.xml	OK
2024-08-10 18:56:06	Parsing APK with androguard	OK
2024-08-10 18:56:06	Extracting Manifest Data	OK
2024-08-10 18:56:06	Performing Static Analysis on: Parental Time Control (com.rockman.dev)	OK
2024-08-10 18:56:06	Fetching Details from Play Store: com.rockman.dev	OK
2024-08-10 18:56:07	Manifest Analysis Started	OK
2024-08-10 18:56:07	Checking for Malware Permissions	OK
2024-08-10 18:56:07	Fetching icon path	OK

2024-08-10 18:56:07	Library Binary Analysis Started	OK
2024-08-10 18:56:07	Reading Code Signing Certificate	OK
2024-08-10 18:56:07	Running APKiD 2.1.5	OK
2024-08-10 18:56:08	Detecting Trackers	OK
2024-08-10 18:56:09	Decompiling APK to Java with jadx	OK
2024-08-10 18:56:12	Converting DEX to Smali	OK
2024-08-10 18:56:12	Code Analysis Started on - java_source	OK
2024-08-10 18:56:13	Android SAST Completed	OK
2024-08-10 18:56:13	Android API Analysis Started	OK
2024-08-10 18:56:15	Android Permission Mapping Started	OK
2024-08-10 18:56:16	Android Permission Mapping Completed	OK
2024-08-10 18:56:16	Finished Code Analysis, Email and URL Extraction	OK
2024-08-10 18:56:16	Extracting String data from APK	OK
2024-08-10 18:56:16	Extracting String data from Code	OK

2024-08-10 18:56:16	Extracting String values and entropies from Code	OK
2024-08-10 18:56:17	Performing Malware check on extracted domains	OK
2024-08-10 18:56:18	Saving to Database	OK

Report Generated by - MobSF v4.0.6

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.