ANDROID STATIC ANALYSIS REPORT

Screen Time (5.3.53)

File Name:	ST Kids App_merged.apk
Package Name:	com.screentime
Scan Date:	Aug. 12, 2024, 7:26 p.m.

App Security Score:	49/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	7/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	28	1	1	1

FILE INFORMATION

File Name: ST Kids App_merged.apk

Size: 7.3MB

MD5: 8bb50db7e4017da265959a2c492b5907

SHA1: 91315c57f94e35cf341a5b9dc3477933574657b6

SHA256: 71e2a1a73606afd061a9aa72bc71bc154e7e22987ed9c9560ee3f925498a1adb

APP INFORMATION

App Name: Screen Time

Package Name: com.screentime

Main Activity: com.screentime.activities.setup.SplashActivity

Target SDK: 33

Min SDK: 19

Max SDK:

Android Version Name: 5.3.53

Android Version Code: 12439

APP COMPONENTS

Activities: 37

Services: 42

Receivers: 52

Providers: 6

Exported Activities: 1

Exported Services: 1

Exported Receivers: 17

Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: C=UK, L=Bristol, CN=Steve Vangasse
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-06-14 16:07:59+00:00
Valid To: 2038-06-08 16:07:59+00:00
Issuer: C=UK, L=Bristol, CN=Steve Vangasse
Serial Number: 0x51bb3fdf
Hash Algorithm: sha1
md5: ceca5f3114f70e1a21c575446230040a
sha1: e689432f7c2a39379bd64cb0bd2a6028f3a666dd
```

sha256: 206f10bfe4f0bee69c3eff56ba9a321854387c9082a3c3be7e2837f55876e1d7

sha512: 47acf6adf3008dac1649d68ab3138f21da2ed26196f6c95b9fa1065c15b3856ba94bbdec54ff67d044a97ad6f53426012d704cdf6e075481b4bd00f135e57e71

PublicKey Algorithm: rsa

Bit Size: 1024

Fingerprint: 74b71b5e2a3699c69fe354f76afe00ffaff443d59ce8c7da7d3a803f8608c546

Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.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.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_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
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.KILL_BACKGROUND_PROCESSES	normal	kill background processes	Allows an application to kill background processes of other applications, even if memory is not low.
com.android.browser.permission.READ_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference

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.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_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
android.permission.INTERACT_ACROSS_USERS	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
com.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.
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.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

APKID ANALYSIS

<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.TAGS check
possible VM 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 Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.screentime,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

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

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **20** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.4-4.4.4, [minSdk=19]	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.screentime.metrics.AttributionReceiver) 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.
3	Broadcast Receiver (com.screentime.BootupBroadcastReceiver) 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.
4	Broadcast Receiver (com.screentime.ShutdownBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Broadcast Receiver (com.screentime.settings.ScreenTimeDeviceAdminReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Broadcast Receiver (com.screentime.domain.time.SystemTimeImpl$TimeChangeReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Broadcast Receiver (com.screentime.android.AndroidSystemStandard$PackageAddedReceiver) 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.
8	Broadcast Receiver (com.screentime.settings.AppLimitsPreferenceFragment$PackageAddedReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Broadcast Receiver (com.screentime.settings.BlockedAppsPreferenceFragment$PackageAddedReceiver) 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	Broadcast Receiver (com.screentime.settings.BedtimeCurfewPreferenceFragment$PackageAddedReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Broadcast Receiver (com.screentime.settings.SchoolCurfewPreferenceFragment$PackageAddedReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Broadcast Receiver (com.screentime.services.sync.DeviceSyncService$PackageAddedReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Broadcast Receiver (com.screentime.services.sync.AppSyncService$PackageAddedReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
14	Broadcast Receiver (com.screentime.android.AndroidSystemDeviceOwner$PackageAddedReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
15	Broadcast Receiver (com.screentime.multiwindow.SamsungMultiWindowStatusReceiver) 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
16	Service (com.screentime.services.accessibility.ScreenTimeAccessibilityService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_ACCESSIBILITY_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.
17	Broadcast Receiver (com.screentime.settings.ScheduleListFragment$PackageAddedReceiver) 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.
18	Broadcast Receiver (com.screentime.android.monitor.photo.MediaStatusBroadcastReceiver) 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 (com.facebook.CustomTabActivity) 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	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.
21	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: **0** | WARNING: **6** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES

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	a3/c.java b0/c.java c5/d.java com/screentime/activities/setup/AccessibilityServiceActivity.java com/screentime/activities/setup/AppUsageActivity.java com/screentime/activities/setup/DrawOverAppsActivity.java com/screentime/activities/setup/IgnoreBatteryOptimizationActivity.java com/screentime/activities/setup/LocationServiceActivity.java com/screentime/activities/setup/ProtectedAppsActivity.java com/screentime/android/i0.java com/screentime/services/logging/LoggingService.java com/screentime/services/recorder/SessionRecorderTask.java com/screentime/services/sync/JobSyncService.java d0/a.java d2/f.java d5/c.java d5/d.java e1/l.java g2/m.java h1/a.java i3/c.java j0/b.java k4/b.java k4/d.java k4/e.java k4/f.java k4/p.java k5/a.java org/joda/time/tz/DateTimeZoneBuilder.java org/joda/time/tz/ZoneInfoCompiler.java r5/b.java s4/a.java s6/h.java t/a.java t4/h.java u5/d.java x/a.java y/a.java y/b.java z2/b.java
2	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	g2/g.java u5/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	y/b.java z2/c.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	c0/a.java com/screentime/db/AppSessionProvider.java com/screentime/db/WebHistoryProvider.java com/screentime/db/a.java n0/a.java n0/c.java n0/d.java
5	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/screentime/domain/time/TimeSyncService.java l6/a.java m6/f.java n3/d.java
6	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	com/screentime/services/recorder/SessionRecorderTask.java
7	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/screentime/android/i0.java
8	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	z2/b.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/24	android.permission.WRITE_SETTINGS, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.GET_TASKS, android.permission.SYSTEM_ALERT_WINDOW, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.WAKE_LOCK, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	7/45	com.google.android.c2dm.permission.RECEIVE, android.permission.PACKAGE_USAGE_STATS, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.FOREGROUND_SERVICE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID

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
firebase-settings.crashlytics.com	ok	**IP:** 142.251.37.3 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
screentimelabs.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
trk.kissmetrics.com	ok	**IP:** 138.197.60.79 **Country:** United States of America **Region:** New Jersey **City:** Clifton **Latitude:** 40.858429 **Longitude:** -74.163757 **View:** Google Map
www.googleapis.com	ok	**IP:** 142.251.36.234 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
storage.googleapis.com	ok	**IP:** 142.251.36.187 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
commons.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
et.kissmetrics.com	ok	**IP:** 138.197.60.79 **Country:** United States of America **Region:** New Jersey **City:** Clifton **Latitude:** 40.858429 **Longitude:** -74.163757 **View:** Google Map
screentimelabs.appspot.com	ok	**IP:** 172.217.16.180 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
console.firebase.google.com	ok	**IP:** 172.217.16.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.youtube.com	ok	**IP:** 142.251.36.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
screentimelabs.com	ok	**IP:** 141.193.213.21 **Country:** United States of America **Region:** Texas **City:** Austin **Latitude:** 30.271158 **Longitude:** -97.741699 **View:** Google Map
www.screentimelabs.com	ok	**IP:** 141.193.213.21 **Country:** United States of America **Region:** Texas **City:** Austin **Latitude:** 30.271158 **Longitude:** -97.741699 **View:** Google Map

FIREBASE DATABASES

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

EMAILS

EMAIL	FILE
correctemail@email.com	com/screentime/activities/setup/SetupPasswordActivity.java
support@screentimelabs.com	m4/b.java
parent@gmail.com eltern@gmail.com genitore@gmail.com correctemail@email.com папамама@gmail.com pais@gmail.com support@screentimelabs.com padre@gmail.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

HARDCODED SECRETS

POSSIBLE SECRETS
"account_disable_all_limiting_key" : "account_disable_all_limiting_key"
"account_disable_bedtime_blocker_key" : "account_disable_bedtime_blocker_key"

POSSIBLE SECRETS
"account_disable_geolocation_activiation_key" : "disable_geolocation_activiation_key"
"account_disable_schedule_blocker_key" : "account_disable_schedule_blocker_key"
"account_disable_scheduled_blockers_key" : "account_disable_scheduled_blockers_key"
"account_disable_schooltime_blocker_key" : "account_disable_schooltime_blocker_key"
"account_geolocation_subs_status_key" : "settings_geolocation_subsstatus"
"account_subs_status_key" : "account_subs_status_key"
"block_temp_unblock_packages_key" : "block_temp_unblock_packages_key"
"block_temp_unblock_until_key" : "block_temp_unblock_until_key"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"facebook_client_token" : "008813fd008edbb0c887abdce19e7df3"
"features_blocked_system_apps_key" : "features_blocked_system_apps_key"
"features_client_logging_enabled_key" : "features_client_logging_enabled_key"
"features_client_logging_min_level_key" : "features_client_logging_min_level_key"
"features_qr_code_enabled_key" : "features_qr_code_enabled_key"
"features_setup_assistance_links_key" : "features_setup_assistance_links_key"
"features_task_kill_devices_key" : "features_task_kill_devices_key"
"features_unlaunchable_whitelist_apps_key" : "features_unlaunchable_whitelist_apps_key"
"features_usage_stats_blacklisted_devices_key" : "features_usage_stats_blacklisted_devices_key"
"features_web_history_enabled_key" : "features_web_history_enabled_key"
"features_web_search_enabled_key" : "features_web_search_enabled_key"
"features_yoda_enabled_key" : "features_yoda_enabled_key"

POSSIBLE SECRETS
"features_yoda_excluded_apps_key" : "features_yoda_excluded_apps_key"
"features_yoda_included_apps_key" : "features_yoda_included_apps_key"
"features_yoda_multipliers_key" : "features_yoda_multipliers_key"
"firebase_database_url" : "https://screentimelabs.firebaseio.com"
"google_api_key" : "AIzaSyDnnoY7I9QOlPDsAD-vd4JxSCS9VOMAjNg"
"google_crash_reporting_api_key" : "AIzaSyDnnoY7I9QOlPDsAD-vd4JxSCS9VOMAjNg"
"is_unsupported_device_key" : "is_unsupported_device"
"rc_did_login_via_token_key" : "did_login_via_token"
"settings_altitude_key" : "altitude"
"settings_app_limit_apps_cat_key" : "app_limit_apps_cat_key"
"settings_app_limit_auto_include_key" : "app_limit_auto_include_key"
"settings_app_limit_default_key" : "default_daily_time_limit"
"settings_app_limit_duration_key" : "settings_app_limit_duration_key"
"settings_app_limit_duration_weekend_key" : "settings_app_limit_duration_weekend_key"
"settings_app_limit_enabled_key" : "app_limit_enabled_key"
"settings_app_limit_included_apps_key" : "settings_app_limit_included_apps_key"
"settings_app_limit_individual_key_prefix" : "app_limit_watch"
"settings_app_limit_warning_key" : "app_limit_warning"
"settings_app_list_select_all_key" : "settings_app_list_select_all_key"
"settings_app_version_key" : "settings_app_version_key"
"settings_bedtime_curfew_apps_cat_key" : "app_bedtime_curfew_cat_key"

POSSIBLE SECRETS
"settings_bedtime_curfew_auto_include_key" : "bedtime_curfew_auto_include_key"
"settings_bedtime_curfew_cache_lights_out_time_key" : "bedtime_curfew_cache_lights_out"
"settings_bedtime_curfew_days_key" : "bedtime_curfew_days"
"settings_bedtime_curfew_enabled_key" : "bedtime_curfew_enabled"
"settings_bedtime_curfew_end_time_key" : "bedtime_curfew_end"
"settings_bedtime_curfew_included_apps_key" : "settings_bedtime_curfew_included_apps_key"
"settings_bedtime_curfew_individual_key_prefix" : "app_bedtime_curfew_watch"
"settings_bedtime_curfew_lights_out_time_key" : "bedtime_curfew_lights_out"
"settings_bedtime_curfew_start_time_key" : "bedtime_curfew_start"
"settings_blocked_apps_auto_include_key" : "blocked_apps_auto_include_key"
"settings_blocked_apps_cat_key" : "blocked_apps_cat_key"
"settings_blocked_apps_enabled_key" : "blocked_apps_enabled"
"settings_blocked_apps_included_apps_key" : "settings_blocked_apps_included_apps_key"
"settings_blocked_apps_individual_key_prefix" : "blocked_apps_enabled_watch"
"settings_curfew_auto_include_key" : "temporary_curfew_auto_include_key"
"settings_device_admin_key" : "key_enable_admin"
"settings_email_key" : "email_address"
"settings_geolocation_enabled_key" : "settings_geolocation_enabled_key"
"settings_ignore_prefix_key" : "ignore_prefix"
"settings_latitude_key" : "latitude"
"settings_light_out_enabled_key" : "light_out_enabled"

POSSIBLE SECRETS
"settings_loc_accuracy_key" : "settings_loc_accuracy"
"settings_loc_provider_key" : "settings_loc_provider"
"settings_loc_timestamp_key" : "settings_loc_timestamp"
"settings_lock_key" : "settings_locked"
"settings_longitude_key" : "longitude"
"settings_password" : "Password"
"settings_password_key" : "password"
"settings_premium_feature_key" : "settings_premium_feture_key"
"settings_rc_activation_code_key" : "settings_rc_activation_code_key"
"settings_rc_activation_code_needed_key" : "settings_rc_activation_code_needed_key"
"settings_rc_child_google_account_key" : "rc_google_account"
"settings_rc_connection_success_key_" : "settings_rc_connection_success_key"
"settings_rc_device_id_key" : "rc_device_id_key"
"settings_rc_device_name_key" : "rc_device_name_key"
"settings_rc_emergency_call_enabled_key" : "settings_rc_emergency_call_enabled_key"
"settings_rc_enabled_switch_key" : "settings_rc_enabled_key"
"settings_rc_gcm_reg_id_key" : "rc_gcm_reg_id"
"settings_rc_last_device_sync_key" : "settings_rc_last_device_sync_key"
"settings_rc_last_session_sync_key" : "settings_rc_last_session_sync_key"
"settings_rc_last_session_sync_start_key" : "settings_rc_last_session_sync_start_key"
"settings_rc_link_key" : "settings_rc_link_key"

POSSIBLE SECRETS
"settings_rc_parent_account_guid_key" : "rc_account_guid"
"settings_rc_parent_account_id_key" : "rc_account_id"
"settings_rc_parent_email_key" : "rc_parent_email_key"
"settings_rc_parent_password_key" : "rc_parent_password_key"
"settings_rc_rapid_sync_until_key" : "settings_rc_rapid_sync_until_key"
"settings_rc_reconnect_key" : "settings_rc_reconnect_key"
"settings_rc_server_screen_state_key" : "settings_rc_server_screen_state_key"
"settings_rc_setup_key" : "settings_rc_setup_key"
"settings_rc_status_key" : "settings_rc_status_key"
"settings_rc_user_id_key" : "rc_user_id_key"
"settings_rc_user_name_key" : "rc_username"
"settings_schedule_curfew_apps_cat_key" : "app_schedule_curfew_cat_key"
"settings_schedule_days_key" : "schedule_days_key"
"settings_schedule_enabled_key" : "schedule_enabled_key"
"settings_schedule_end_time_key" : "schedule_end"
"settings_schedule_id_key" : "schedule_id_key"
"settings_schedule_included_apps_key" : "schedule_included_apps_key"
"settings_schedule_name_key" : "schedule_name_key"
"settings_schedule_start_time_key" : "schedule_start"
"settings_school_curfew_apps_cat_key" : "app_school_curfew_cat_key"
"settings_school_curfew_auto_include_key" : "school_curfew_auto_include_key"

POSSIBLE SECRETS
"settings_school_curfew_enabled_key" : "school_curfew_enabled"
"settings_school_curfew_end_time_key" : "school_curfew_end"
"settings_school_curfew_included_apps_key" : "settings_school_curfew_included_apps_key"
"settings_school_curfew_individual_key_prefix" : "app_school_curfew_watch"
"settings_school_curfew_start_time_key" : "school_curfew_start"
"settings_system_time_key" : "settings_system_time_key"
"settings_system_time_zone_key" : "settings_system_time_zone_key"
"settings_temporary_curfew_apps_cat_key" : "app_temporary_curfew_cat_key"
"settings_temporary_days_key" : "temporary_days_key"
"settings_temporary_enabled_key" : "temporary_enabled_key"
"settings_temporary_end_time_key" : "temporary_end"
"settings_temporary_included_apps_key" : "temporary_included_apps_key"
"settings_temporary_name_key" : "temporary_name_key"
"settings_temporary_prefix_key" : "temporary_prefix"
"settings_temporary_start_time_key" : "temporary_start"
"settings_web_filtering_account_enabled_key" : "wf_account_enabled"
"settings_web_filtering_banned_categories_key" : "wf_categories"
"settings_web_filtering_blacklist_fqdns_key" : "wf_blacklist_fqdns"
"settings_web_filtering_network_verifier_usable_key" : "wf_netstat_usable"
"settings_web_filtering_user_enabled_key" : "wf_user_enabled"
"settings_web_filtering_whitelist_fqdns_key" : "wf_whitelist_fqdns"

POSSIBLE SECRETS
"settings_password" : "Passwort"
"settings_password" : "Contraseña"
"settings_password" : "Password"
"settings_password" : "□□□□"
"settings_password" : "Senha"
"settings_password" : "Пароль"
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b>□□□□□□□□□□□□□□□□□□□□□□□□"
"com_facebook_device_auth_instructions" : "□□<b>facebook.com/device</b>□□□□□□□□□□□□"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
9b8f518b086098de3d77736f9458a3d2f6f95a37
f7921b18af76691d1ab7448109b6dd13
51cf571d8cd0729783bbfe1e0400739b
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
9e08b56f8e96592ae48ed58d82366e71
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
cc2751449a350f668590264ed76692694a80308a
c56fb7d591ba6704df047fd98f535372fea00211
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
5509619a5433b408ecdf5921f0fef1fae9a3dbc0
470fa2b4ae81cd56ecbcda9735803434cec591fa

POSSIBLE SECRETS
e54a00e8a1e00360c517b2f7c39162ae
67a3e3eada9f6b7d669c4244c5d214f5
aab3a5a1a4777011eba709b897dfc055

PLAYSTORE INFORMATION

Title: ST Kids App

Score: 1.5758514 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Tools **Play Store URL:** com.screentime

Developer Details: Parental Control App by Screen Time Labs, 4922207927270705654, Screen Time Labs LTD 1391 Post Rd. E. Westport, CT 06880, https://screentimelabs.com, support@screentimelabs.com,

Release Date: Jun 14, 2013 **Privacy Policy:** Privacy link

Description:

Screen Time for Kids works in conjunction with the Screen Time Parental Control App on your child's device. This app uses Accessibility services. Screen Time requires accessibility permissions to monitor and limit daily screen time usage. Specifically, Accessibility services are required for: • App blocking both on-demand and schedule based blocking on kid’s devices. • Web monitoring to capture web history on kid’s devices. • Web filtering to keep kids safe while browsing online. This is important to support all children, including those with pre-diagnosed disabilities, from creating or aggravating social, learning and other behavioral disorders. Privacy Policy You can review the full Privacy Policy here. Feedback If you have any problems please take a look at our help pages, or contact us via the contact page of our website, since we cannot always help you if you post questions in the reviews. https://screentimelabs.com/help https://screentimelabs.com/contact This app uses the Device Administrator permission.

SCAN LOGS

Timestamp	Event	Error
2024-08-12 19:26:35	Generating Hashes	OK
2024-08-12 19:26:35	Extracting APK	OK
2024-08-12 19:26:35	Unzipping	OK
2024-08-12 19:26:35	Getting Hardcoded Certificates/Keystores	OK
2024-08-12 19:26:37	Parsing AndroidManifest.xml	OK

2024-08-12 19:26:37	Parsing APK with androguard	OK
2024-08-12 19:26:37	Extracting Manifest Data	OK
2024-08-12 19:26:37	Performing Static Analysis on: Screen Time (com.screentime)	OK
2024-08-12 19:26:37	Fetching Details from Play Store: com.screentime	OK
2024-08-12 19:26:38	Manifest Analysis Started	OK
2024-08-12 19:26:38	Checking for Malware Permissions	OK
2024-08-12 19:26:38	Fetching icon path	OK
2024-08-12 19:26:38	Library Binary Analysis Started	OK
2024-08-12 19:26:38	Reading Code Signing Certificate	OK
2024-08-12 19:26:38	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/8bb50db7e4017da265959a2c492b5907/8bb50db7e4017da265959a2c492b5907.apk'])
2024-08-12 19:26:38	Running APKiD 2.1.5	OK
2024-08-12 19:26:40	Detecting Trackers	OK
2024-08-12 19:26:41	Decompiling APK to Java with jadx	OK
2024-08-12 19:27:00	Converting DEX to Smali	OK

2024-08-12 19:27:00	Code Analysis Started on - java_source	OK
2024-08-12 19:28:49	Android SAST Completed	OK
2024-08-12 19:28:49	Android API Analysis Started	OK
2024-08-12 19:30:32	Android Permission Mapping Started	OK
2024-08-12 19:31:19	Android Permission Mapping Completed	OK
2024-08-12 19:31:20	Finished Code Analysis, Email and URL Extraction	OK
2024-08-12 19:31:20	Extracting String data from APK	OK
2024-08-12 19:31:20	Extracting String data from Code	OK
2024-08-12 19:31:20	Extracting String values and entropies from Code	OK
2024-08-12 19:31:22	Performing Malware check on extracted domains	OK
2024-08-12 19:31:24	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.