



## ANDROID STATIC ANALYSIS REPORT



 Mobile Fence (5.6.2)

File Name:

base.apk

Package Name:

com.mobilefence.family

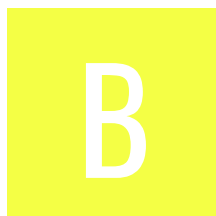
Scan Date:

Aug. 18, 2024, 11:16 a.m.

App Security Score:






43/100 (MEDIUM RISK)

Grade:



Trackers Detection:

2/432

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
5	24	1	1	1

## FILE INFORMATION

**File Name:** base.apk

**Size:** 15.36MB

**MD5:** c7dddb5413ef1c30319cf0a2b6138032

**SHA1:** acf53cbb8762f002f6b636b5221cba408d97ae02

**SHA256:** c0ee676ae751aa1332e0e80b5bea4a657e78a837fdea94b430978afaa9e958f3

## APP INFORMATION

**App Name:** Mobile Fence

**Package Name:** com.mobilefence.family

**Main Activity:** com.mobilefence.family.IntroActivity

**Target SDK:** 34

**Min SDK:** 21

**Max SDK:**

**Android Version Name:** 5.6.2

**Android Version Code:** 474

## APP COMPONENTS

**Activities:** 44

**Services:** 13

**Receivers:** 24

**Providers:** 4

**Exported Activities:** 1

**Exported Services:** 2

**Exported Receivers:** 7

# CERTIFICATE INFORMATION

Binary is signed  
v1 signature: True  
v2 signature: True  
v3 signature: False  
v4 signature: False  
X.509 Subject: C=US, ST=LA, L=CA, O=Mobile Fence, OU=Mobile Fence, CN=mobilefence  
Signature Algorithm: rsassa\_pkcs1v15  
Valid From: 2014-10-12 00:34:47+00:00  
Valid To: 2042-02-27 00:34:47+00:00  
Issuer: C=US, ST=LA, L=CA, O=Mobile Fence, OU=Mobile Fence, CN=mobilefence  
Serial Number: 0x920b2ab  
Hash Algorithm: sha256  
md5: 4db58aea77808af336766cba70e4307e  
sha1: bb7fd749c0e7005a8b91bfc172e553c09a24b53e  
sha256: 8c59d6f6f5160a604ff2fe64f57316d03be766fdda7667bfaadabee16959b5ae  
sha512: 4f46cb2026bacec14b1ca1d14963579a145d62ef7da76268777fbefc9c6c735877d88494b279b3c092254f63ee6ff65e22436cad4ae0f0dccfaf14a24e261430  
PublicKey Algorithm: rsa  
Bit Size: 2048  
Fingerprint: d92b0fb1e0be4c1e78bc9484f113189bc29496e42cd50a2f05fb89b2b54b7058  
Found 1 unique certificates

## APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.mobilefence.family.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
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.

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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.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.DISABLE_KEYGUARD	normal	disable keyguard	Allows applications to disable the keyguard if it is not secure.

PERMISSION	STATUS	INFO	DESCRIPTION
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_PHONE_NUMBERS	dangerous	allows reading of the device's phone number(s).	Allows read access to the device's phone number(s). This is a subset of the capabilities granted by READ_PHONE_STATE but is exposed to instant applications.
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.
com.android.browser.permission.READ_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference
com.android.browser.permission.WRITE_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
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.
android.permission.EXPAND_STATUS_BAR	normal	expand/collapse status bar	Allows application to expand or collapse the status bar.
android.permission.DIAL_PHONE	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
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.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_SYSTEM_EXEMPTED	normal	allows system-exempted types of foreground services.	Allows a regular application to use Service.startForeground with the type "systemExempted". Apps are allowed to use this type only in the use cases listed in ServiceInfo.FOREGROUND_SERVICE_TYPE_SYSTEM_EXEMPTED.
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.QUERY_ALL_PACKAGES	normal	enables querying any normal app on the device.	Allows query of any normal app on the device, regardless of manifest declarations.
android.permission.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.
android.permission.READ_MEDIA_AUDIO	dangerous	allows reading audio files from external storage.	Allows an application to read audio files from external storage.
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.
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.mobilefence.family.permission.ADDON_COMM	unknown	Unknown permission	Unknown permission from android reference
com.mobilefence.family.permission.PLUGIN_COMM	unknown	Unknown permission	Unknown permission from android reference
com.samsung.android.knox.permission.KNOX_RESTRICTION_MGMT	unknown	Unknown permission	Unknown permission from android reference
com.samsung.android.knox.permission.KNOX_ENTERPRISE_DEVICE_ADMIN	unknown	Unknown permission	Unknown permission from android reference
com.samsung.android.knox.permission.KNOX_SECURITY	unknown	Unknown permission	Unknown permission from android reference
com.samsung.android.knox.permission.KNOX_LOCATION	unknown	Unknown permission	Unknown permission from android reference



PERMISSION	STATUS	INFO	DESCRIPTION
com.samsung.android.knox.permission.KNOX_INVENTORY	unknown	Unknown permission	Unknown permission from android reference
com.samsung.android.knox.permission.KNOX_PHONE_RESTRICTION	unknown	Unknown permission	Unknown permission from android reference
com.samsung.android.knox.permission.KNOX_APP_MGMT	unknown	Unknown permission	Unknown permission from android reference
com.samsung.android.knox.permission.KNOX_HW_CONTROL	unknown	Unknown permission	Unknown permission from android reference
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.ACCESS_AD_SERVICES_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_AD_SERVICES_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.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.mobidefence.family.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check
	Compiler	r8 without marker (suspicious)
classes2.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.TAGS check
	Compiler	r8 without marker (suspicious)

FILE	DETAILS	
classes3.dex	FINDINGS	DETAILS
	Anti Debug Code	Debug.isDebuggerConnected() check
	Anti-VM Code	Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check possible VM check
	Compiler	r8 without marker (suspicious)
assets/MF_Family_Addon_LG.apk!classes.dex	FINDINGS	DETAILS
	Compiler	dx
assets/MF_Family_Plugin.apk!classes.dex	FINDINGS	DETAILS
	Compiler	r8

## BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.navercorp.nid.oauth.activity.NidOAuthCustomTabActivity	Schemes: naver3rdpartylogin://, Hosts: authorize, Paths: /,

## 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
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.

## MANIFEST ANALYSIS

HIGH: 2 | WARNING: 14 | 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	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Broadcast Receiver (com.mobilefence.family.receiver.SimStateChangedReceiver) 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	Service (com.mobilefence.family.service.MdmService) is Protected by a permission. Permission: com.mobilefence.family.permission.FAMILY_COMM_SIGNATURE protectionLevel: signature [android:exported=true]	info	A Service is found to be exported, but is protected by permission.
5	Service (com.mobilefence.family.service.TempService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.mobilefence.family.permission.FAMILY_COMM protectionLevel: normal [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. However, the protection level of the permission is set to normal. This means that a malicious application can request and obtain the permission and interact with the component. If it was set to signature, only applications signed with the same certificate could obtain the permission.
6	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
7	Broadcast Receiver (com.mobilefence.core.knox.KnoxLicenseReceiver) 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	Content Provider (com.mobilefence.family.provider.SharedSettingsProvider) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.mobilefence.family.permission.FAMILY_COMM protectionLevel: normal [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission. However, the protection level of the permission is set to normal. This means that a malicious application can request and obtain the permission and interact with the component. If it was set to signature, only applications signed with the same certificate could obtain the permission.
9	Broadcast Receiver (com.mobilefence.family.receiver.AddonCommunicator) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.mobilefence.family.permission.FAMILY_COMM protectionLevel: normal [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. However, the protection level of the permission is set to normal. This means that a malicious application can request and obtain the permission and interact with the component. If it was set to signature, only applications signed with the same certificate could obtain the permission.
10	Broadcast Receiver (com.mobilefence.family.receiver.SACReceiver) 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.samsung.android.knox.IntentConverterReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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
13	Activity (com.navercorp.nid.oauth.activity.NidOAuthCustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
14	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 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.
15	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
16	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
17	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: 3 | WARNING: 7 | INFO: 1 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
----	-------	----------	-----------	-------

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	<a href="#">Files may contain hardcoded sensitive information like usernames, passwords, keys etc.</a>	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/bumptech/glide/load/engine/d.java com/bumptech/glide/load/engine/p.java com/bumptech/glide/load/engine/x.java com/bumptech/glide/load/i.java com/mobilefence/family/MainActivity.java com/mobilefence/family/helper/t.java com/samsung/android/knox/accounts/Account.java com/samsung/android/knox/accounts/HostAuth.java u/n.java
				com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/q.java com/airbnb/lottie/utils/e.java com/bumptech/glide/c.java com/bumptech/glide/gifdecoder/e.java com/bumptech/glide/gifdecoder/g.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/load/data/mediastore/c.java com/bumptech/glide/load/data/mediastore/e.java com/bumptech/glide/load/engine/bitmap_recycle/j.java com/bumptech/glide/load/engine/bitmap_recycle/l.java com/bumptech/glide/load/engine/cache/e.java com/bumptech/glide/load/engine/cache/l.java com/bumptech/glide/load/engine/executor/a.java com/bumptech/glide/load/engine/executor/b.java com/bumptech/glide/load/engine/h.java com/bumptech/glide/load/engine/i.java com/bumptech/glide/load/engine/k.java com/bumptech/glide/load/engine/prefill/a.java com/bumptech/glide/load/engine/q.java com/bumptech/glide/load/engine/z.java com/bumptech/glide/load/model/c.java



NO	ISSUE	SEVERITY	STANDARDS	FILES
2	<a href="#">The App logs information. Sensitive information should never be logged.</a>	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/bumptechn/glide/load/model/d.java com/bumptechn/glide/load/model/f.java com/bumptechn/glide/load/model/s.java com/bumptechn/glide/load/model/t.java com/bumptechn/glide/load/resource/bitmap/c0.java com/bumptechn/glide/load/resource/bitmap/e.java com/bumptechn/glide/load/resource/bitmap/g0.java com/bumptechn/glide/load/resource/bitmap/m.java com/bumptechn/glide/load/resource/bitmap/p.java com/bumptechn/glide/load/resource/bitmap/q.java com/bumptechn/glide/load/resource/bitmap/v.java com/bumptechn/glide/load/resource/gif/a.java com/bumptechn/glide/load/resource/gif/d.java com/bumptechn/glide/load/resource/gif/j.java com/bumptechn/glide/manager/e.java com/bumptechn/glide/manager/f.java com/bumptechn/glide/manager/k.java com/bumptechn/glide/manager/m.java com/bumptechn/glide/manager/o.java com/bumptechn/glide/manager/p.java com/bumptechn/glide/module/e.java com/bumptechn/glide/request/j.java com/bumptechn/glide/request/target/f.java com/bumptechn/glide/request/target/r.java com/bumptechn/glide/signature/a.java com/bumptechn/glide/util/c.java com/bumptechn/glide/util/pool/a.java com/mobilefence/core/util/b1.java com/mobilefence/core/util/f0.java com/mobilefence/core/util/h0.java com/mobilefence/core/util/p0.java com/mobilefence/core/util/s0.java com/mobilefence/core/util/x0.java com/samsung/android/knox/EnterpriseDeviceManager.java com/samsung/android/knox/EnterpriseKnoxManager.java com/samsung/android/knox/container/ContainerModeConfigurationType.java

NO	ISSUE	SEVERITY	STANDARDS	com/samsung/android/knox/container/KnoxConfigurationType.java com/samsung/android/knox/container/KnoxContainerManager.java com/samsung/android/knox/container/LightweightConfigurationType.java com/samsung/android/knox/custom/CustomDeviceManager.java com/samsung/android/knox/integrity/AttestationPolicy.java com/samsung/android/knox/license/EnterpriseLicenseManager.java com/samsung/android/knox/license/KnoxEnterpriseLicenseManager.java com/samsung/android/knox/log/AuditLog.java com/samsung/android/knox/net/vpn/KnoxONVpnService.java com/samsung/android/knox/sdp/SdpUtil.java com/samsung/android/knox/sdp/core/SdpEngine.java com/samsung/android/knox/seams/SEAMSPolicy.java com/samsung/android/knox/ucm/configurator/UniversalCredentialManager.java com/samsung/android/knox/ucm/core/SecureChannelManager.java com/samsung/android/knox/ucm/core/UniversalCredentialUtil.java com/yalantis/ucrop/UCropActivity.java com/yalantis/ucrop/task/BitmapCropTask.java com/yalantis/ucrop/task/BitmapLoadTask.java com/yalantis/ucrop/util/BitmapLoadUtils.java com/yalantis/ucrop/util/EglUtils.java com/yalantis/ucrop/util/FileUtils.java com/yalantis/ucrop/util/ImageHeaderParser.java com/yalantis/ucrop/view/TransformImageView.java h/a.java p1/b.java y/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	<a href="#">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.</a>	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	t/a.java t/c.java t/d.java t/f.java t/g.java t/i.java t/j.java t/k.java t/l.java
4	<a href="#">App can read/write to External Storage. Any App can read data written to External Storage.</a>	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/livechatinc/inappchat/UriUtils.java com/mobilefence/core/util/x.java com/mobilefence/family/helper/e.java com/samsung/android/knox/sdp/SdpFileSyste m.java com/yalantis/ucrop/util/FileUtils.java
5	<a href="#">The App uses an insecure Random Number Generator.</a>	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/mobilefence/core/util/e1.java com/mobilefence/core/util/x.java com/mobilefence/family/helper/d.java com/mobilefence/family/helper/f.java com/mobilefence/family/helper/k.java x0/a.java
6	<a href="#">The file or SharedPreferences is World Readable. Any App can read from the file</a>	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/mobilefence/core/util/h.java
7	<a href="#">This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.</a>	secure	OWASP MASVS: MSTG-NETWORK-4	com/mobilefence/core/util/p0.java
8	<a href="#">Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.</a>	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/livechatinc/inappchat/ChatWindowView.ja va com/mobilefence/core/util/x.java com/mobilefence/family/WebViewFragment.ja va

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	<a href="#">Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks</a>	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/mobilefence/core/util/x.java com/mobilefence/family/UserRegistrationActivity.java com/mobilefence/family/WebViewFragment.java
10	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/mobilefence/family/foundation/c.java
11	<a href="#">MD5 is a weak hash known to have hash collisions.</a>	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/mobilefence/family/util/f.java
12	<a href="#">The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.</a>	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/mobilefence/family/util/e.java

## NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

## ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	15/24	android.permission.RECEIVE_BOOT_COMPLETED, android.permission.GET_TASKS, android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.GET_ACCOUNTS, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.SYSTEM_ALERT_WINDOW, android.permission.READ_PHONE_STATE, android.permission.READ_CONTACTS, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	13/45	com.google.android.c2dm.permission.RECEIVE, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.CHANGE_WIFI_STATE, android.permission.CALL_PHONE, android.permission.PACKAGE_USAGE_STATS, com.google.android.gms.permission.ACTIVITY_RECOGNITION, android.permission.ACTIVITY_RECOGNITION, android.permission.ACCESS_NOTIFICATION_POLICY, android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, 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
dapi.kakao.com	ok	IP: 121.53.104.36 Country: Korea (Republic of) Region: Seoul-teukbyeolsi City: Seoul Latitude: 37.568260 Longitude: 126.977829 View: <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	<b>IP:</b> 142.251.37.4 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
m.vguard.co.kr	ok	No Geolocation information available.
www.asdasdadsadfasdf.com	ok	No Geolocation information available.
cdn.livechat-files.com	ok	<b>IP:</b> 95.101.23.96 <b>Country:</b> Austria <b>Region:</b> Wien <b>City:</b> Vienna <b>Latitude:</b> 48.208488 <b>Longitude:</b> 16.372080 <b>View:</b> <a href="#">Google Map</a>
www.example.com	ok	<b>IP:</b> 93.184.215.14 <b>Country:</b> United States of America <b>Region:</b> Virginia <b>City:</b> Ashburn <b>Latitude:</b> 39.043720 <b>Longitude:</b> -77.487488 <b>View:</b> <a href="#">Google Map</a>
javax.xml.xmlconstants	ok	No Geolocation information available.
www.mobilefence.com	ok	<b>IP:</b> 54.144.127.117 <b>Country:</b> United States of America <b>Region:</b> Virginia <b>City:</b> Ashburn <b>Latitude:</b> 39.043720 <b>Longitude:</b> -77.487488 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	<b>IP:</b> 142.251.36.206 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
www.facebook.com	ok	<b>IP:</b> 31.13.84.36 <b>Country:</b> Austria <b>Region:</b> Wien <b>City:</b> Vienna <b>Latitude:</b> 48.208488 <b>Longitude:</b> 16.372080 <b>View:</b> <a href="#">Google Map</a>
nid.naver.com	ok	<b>IP:</b> 203.104.163.42 <b>Country:</b> Germany <b>Region:</b> Hessen <b>City:</b> Frankfurt am Main <b>Latitude:</b> 50.115520 <b>Longitude:</b> 8.684170 <b>View:</b> <a href="#">Google Map</a>
www.googleadservices.com	ok	<b>IP:</b> 172.217.16.162 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
cdn.livechatinc.com	ok	<b>IP:</b> 95.101.23.96 <b>Country:</b> Austria <b>Region:</b> Wien <b>City:</b> Vienna <b>Latitude:</b> 48.208488 <b>Longitude:</b> 16.372080 <b>View:</b> <a href="#">Google Map</a>
openapi.naver.com	ok	<b>IP:</b> 110.93.147.11 <b>Country:</b> Korea (Republic of) <b>Region:</b> Gyeonggi-do <b>City:</b> Seongnam <b>Latitude:</b> 37.438610 <b>Longitude:</b> 127.137779 <b>View:</b> <a href="#">Google Map</a>
latvia-719.firebaseio.com	ok	<b>IP:</b> 35.201.97.85 <b>Country:</b> United States of America <b>Region:</b> Missouri <b>City:</b> Kansas City <b>Latitude:</b> 39.099731 <b>Longitude:</b> -94.578568 <b>View:</b> <a href="#">Google Map</a>

## FIREBASE DATABASES

FIREBASE URL	DETAILS
https://latvia-719.firebaseio.com	<a href="#">info</a> App talks to a Firebase Database.

## EMAILS



EMAIL	FILE
kimhwan97@gmail.com	com/mobilefence/family/BlockScreenActivity.java
kimhwan97@gmail.com	com/mobilefence/family/UserLoginActivity.java
w+@gmail.com w+@googlemail.com	com/mobilefence/core/util/e1.java
myid@address.com youremail@gmail.com	Android String Resource

## TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	<a href="https://reports.exodus-privacy.eu.org/trackers/27">https://reports.exodus-privacy.eu.org/trackers/27</a>
Google Firebase Analytics	Analytics	<a href="https://reports.exodus-privacy.eu.org/trackers/49">https://reports.exodus-privacy.eu.org/trackers/49</a>

## HARDCODED SECRETS

POSSIBLE SECRETS
"col_auth_title" : "Login"
"col_user_name" : "Name"
"com.google.firebase.crashlytics.mapping_file_id" : "16480e369cdf49f7954ce6e33f799990"
"firebase_database_url" : "https://latvia-719.firebaseio.com"

POSSIBLE SECRETS
"ga_cate_user" : "User"
"google_api_key" : "AlzaSyAmoyXTctowsa6d0gniRFspkjsxnilxMaEA"
"google_crash_reporting_api_key" : "AlzaSyAmoyXTctowsa6d0gniRFspkjsxnilxMaEA"
"col_add_user" : "□□□□"
"col_auth_done_title" : "□□□□"
"col_auth_title" : "□□□□"
"col_remember_pwd" : "□□□□□□□□"
"col_switch_user" : "□□□□□□□□□□□□□□"
"col_user_name" : "□□"
"err_login_no_auth" : "□□□□□□□□□□□□□□□□"
"col_auth_title" : "Anmelden"
"col_user_name" : "Name"
"col_auth_title" : "□□□□"
"col_user_name" : "□□"
"col_auth_title" : "Identifiant"
"col_user_name" : "Nom"
"col_user_name" : "Nombre"
"col_auth_title" : "Login"

POSSIBLE SECRETS
"col_user_name" : "Nome"
"col_auth_title" : "Логин"
"col_user_name" : "Имя"
"naveroauthlogin_string_token_invalid" : "aaaaaaaaaaaaaaaa"
"naveroauthlogin_string_token_invalid" : "aaaaaaaaaaaaaaaa"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
Y29tLmtha2FvLnRhbGsuYWN0aXZpdHkuYnJvd3Nlci5JbkFwcEjyb3dzZXJBY3Rpdml0eQ==
Y29tLmFuZHJvaWQucGFja2FnZWluc3RhbGxlcj5wZXJtaXNzaW9uLnVpLjJldmllZD1Blcm1pc3Npb25zQWN0aXZpdHk=
Y29tLmdvb2dsZS5hbmRyb2lkLnlvdXR1YmU6aWQvcmlvF9tYWluX3RpdGxl
Y29tLmdvb2dsZS5hbmRyb2lkLmdvb2dsZXF1aWNrc2VhcmNoYm94
Y29tLmVzdHNvZnQuYWx5YWModGFibGV0
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
5ed7bf382997eb4406c42c9484dcfcae
a3MuY20uYW50aXZpcnVzLnByaXZhdGVicm93c2luZw==
Y29tLmdvb2dsZS5hbmRyb2lkLmFwcHMueW91dHVlZS5hcHAuc2V0dGluZ3MuU2V0dGluZ3NBY3Rpdml0eQ==
b3JnLmNocm9taXVtLmNocm9tZS5icm93c2VyLmN1c3RvbXRhYnMuU2VwYXJhdGVUYXNrQ3VzdG9tVGFiQWN0aXZpdHk=
470fa2b4ae81cd56ecbcda9735803434cec591fa
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319



POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
Y29tLmFuZHJvaWQuY2hyb21lOmklL3VybfF9iYXI=
Y29tLmj1enpwaWEuYXF1YS5sYXVuY2hlcj5hcHAuc2VydmljZS53ZWluSG9tZXBhY2tidXp6QWN0aXZpdHk=
Y29tLmdvb2dsZS5hbmRyb2lkLmFwcHMuc2N3LnNlYXJjaG5vdy5TZWFyY2hOb3dBY3Rpdml0eQ==
Y29tLmFuZHJvaWQubW1zOmklL2ljX2Nsb3NlX3g=
Y29tLmtha2FvLmhvbWUua2FrYW9fc2VhcmNoLktha2FvQnJvd3NlckFjdGl2aXR5
Y29tLmZhY2Vib29rLmJyb3dzZXlubGl0ZS5Ccm93c2VyTGl0ZUFjdGl2aXR5
Y29tLmtha2FvLnRhbGsuZ2FtZXRhYi52aWV3LkdhbWV0YWJQb3B1cEFjdGl2aXR5
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
Y29tLmj1enpwaWEuYXF1YS5sYXVuY2hlcg==
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
anAubmF2ZXlubGluZS5hbmRyb2lkLmFjdGl2aXR5LmlhYi5JbkFwcEjyb3dzZXJBY3Rpdml0eQ==
Y29tLmtha2FvLmhvbWUua2FrYW9fc2VhcmNoLktha2FvU2VhcmNoQWN0aXZpdHk=
Y29tLmFuZHJvaWQuc2V0dGluZ3MuRGV2aWNIQWRtaW5BZGQ=
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
Y29tLmNhbxXbt2JpbGUubGF1bmNoZXluaG9tZS5zZWlyY2guU2VhcmNoQWN0aXZpdHk=

POSSIBLE SECRETS
258EAFa5-E914-47DA-95CA-C5AB0DC85B11
Y29tLmtha2FvLnRhbGsuYWN0aXZpdHkuY2hhdC5JbkFwcEjyb3dzZXJBY3Rpdml0eQ==
Y29tLmdvb2dsZS5hbmRyb2lkLnldXR1YmU6aWQvcGxheWxpc3RfcGFuZWxfdmkZW9faXRlbQ==
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
Y29tLmdvb2dsZS5hbmRyb2lkLmFwcHMueW91dHVlZS5hcHAuaG9uZXljb21iLlNldHRpbmdzQWN0aXZpdHk=
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
Y29tLmppdWJhbmcuYnVzc2luZXNzY2VudGVyLnBsdWdpbi5uYXZpZ2F0aW9ucGFuZS5jb21tb24ud2ViLldlYlZpZXdB3Rpdml0eQ==
Y29tLmtzbW9iaWxILmJ1c2luZXNzLnNkay5zZWYyY2gud2Vidmlldy5TZWFyY2hXZWJWaWV3QWN0aXZpdHk=
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
Y29tLmdvb2dsZS5hbmRyb2lkLnldXR1YmU6aWQvc2VhcmNoX3F1ZXJ5
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

## PLAYSTORE INFORMATION

**Title:** MobileFence - Parental Control

**Score:** 3.1423357 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Parenting **Play Store URL:** [com.mobilefence.family](https://play.google.com/store/apps/details?id=com.mobilefence.family)

**Developer Details:** Mobile Fence, Mobile+Fence, 800 West El Camino Real, Suite 180, Mountain View, California, 94040, <http://www.mobilefence.com>, [user-support@mobilefence.com](mailto:user-support@mobilefence.com),

**Release Date:** Mar 16, 2015 **Privacy Policy:** [Privacy link](#)

### Description:

Mobile Fence Parental Control protects children from accessing harmful contents (websites, apps, videos) through smart devices and limits usage time to prevent smartphone addiction. Also, parents can monitor their children's location in real time and is notified when their children enters or leaves safety zone set by the parents. "Help your children enjoy their mobile device

safely!" Child Protection Software. Main Functions ✓ App Blocking - Protect your child against harmful apps. Parents can control and block unwanted apps(adult, dating, pornography, games, SNS..) or set time limits. ✓ WebSite Blocking (Safe Browsing) - Protect your child from unsuitable web content. Parents can block access to harmful contents or inappropriate sites, such as adult/nude/pornography websites, and monitor list of websites they visited. ✓ Game Play Time - Protect your children from game addiction. Parent can set how long your child can play games in a day. ✓ Planning Device Time - Protect your children from smartphone addiction. Plan a specific time limit for each day of the week to prevent your kids from late-night games, web browsing, SNS. ✓ Geo Fencing - Parents can track location of their kids in case of kidnapping and receive notification when a child enters or leaves the safety zone set by the parents. ✓ Monitor all activities - Parents can view their child's entire online activities, such as device usage time, frequently launched apps, app usage time, visited website, calls & SMS ✓ Call Block - Block unwanted calls, set a list of allowed callers ✓ Keyword Alerts - When a child receives a text including a key words parents have set, it notifies parents immediately so that parents can actively respond to violence and bullying at school. ✓ Block while walking (Prevent Smart Phone Zombie) How to use 1) Install Mobile Fence on parent's smart device 2) Create account and login 3) Link the smart device to Mobile Fence 4) Installation complete 5) Launch Mobile Fence and set family rules. How to install and link Mobile Fence Parental Control to child's device 1) Install Mobile Fence to child's device 2) Login with parent's account 3) Link Mobile Fence with child's device Functions • Blocking Service - Block apps, Block website(Safe Browsing), Location tracking, game time limiting, harmful content block(Child Protection), Call Block • Monitoring Service - Launched app, Visited Website, Blocked website, Usage time report, Frequently used app report • Call/Text Service - Call block, Text message monitoring, Keyword Alert, Adult/International call block • Location Tracking - Child location tracking, Lost device tracking, Remote factory reset, Remote device control, Geo Fencing, Geo Watching ----- Mobile Fence Parental Control : <http://www.mobilefence.com> Facebook : <http://www.facebook.com/MobileFence> ----- # This app uses the Device Administrator permission. # This app uses Accessibility services. # This app collects health information for the "block smartphone while walking" function. # This app collects and transmits the following personal information to the server, processes this information and provides it to parents: phone number, device ID, device location, device app list, fitness information, visited website. # Notice of use of Accessibility Service API The Mobile Fence app uses Accessibility Service API for the following purposes. The monitored data is sent to the server to provide data to parents. - Monitor your child's visited websites - Block harmful adult sites - Fitness information for blocking while walking - Collection of location information for child location reporting function - A device unique identifier

## SCAN LOGS

Timestamp	Event	Error
2024-08-18 11:16:34	Generating Hashes	OK
2024-08-18 11:16:34	Extracting APK	OK
2024-08-18 11:16:34	Unzipping	OK
2024-08-18 11:16:35	Getting Hardcoded Certificates/Keystores	OK
2024-08-18 11:16:37	Parsing AndroidManifest.xml	OK

2024-08-18 11:16:37	Parsing APK with androguard	OK
2024-08-18 11:16:38	Extracting Manifest Data	OK
2024-08-18 11:16:38	Performing Static Analysis on: Mobile Fence (com.mobilefence.family)	OK
2024-08-18 11:16:38	Fetching Details from Play Store: com.mobilefence.family	OK
2024-08-18 11:16:38	Manifest Analysis Started	OK
2024-08-18 11:16:38	Checking for Malware Permissions	OK
2024-08-18 11:16:38	Fetching icon path	OK
2024-08-18 11:16:38	Library Binary Analysis Started	OK
2024-08-18 11:16:38	Reading Code Signing Certificate	OK
2024-08-18 11:16:39	Running APKID 2.1.5	OK
2024-08-18 11:16:42	Detecting Trackers	OK
2024-08-18 11:16:45	Decompiling APK to Java with jadx	OK



2024-08-18 11:17:20	Converting DEX to Smali	OK
2024-08-18 11:17:20	Code Analysis Started on - java_source	OK
2024-08-18 11:18:40	Android SAST Completed	OK
2024-08-18 11:18:40	Android API Analysis Started	OK
2024-08-18 11:19:49	Android Permission Mapping Started	OK
2024-08-18 11:23:20	Android Permission Mapping Completed	OK
2024-08-18 11:23:21	Finished Code Analysis, Email and URL Extraction	OK
2024-08-18 11:23:21	Extracting String data from APK	OK
2024-08-18 11:23:22	Extracting String data from Code	OK
2024-08-18 11:23:22	Extracting String values and entropies from Code	OK
2024-08-18 11:23:25	Performing Malware check on extracted domains	OK
2024-08-18 11:23:27	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.

© 2024 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).