

ANDROID STATIC ANALYSIS REPORT



MTG Familiar (3.6.6.dbg.3)

File Name:	installer379.apk	
Package Name:	com.gelakinetic.mtgfam	
Scan Date:	May 31, 2022, 3:11 p.m.	
App Security Score:	47/100 (MEDIUM RISK)	
Grade:		

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	ℚ HOTSPOT
2	11	2	1	1

FILE INFORMATION

File Name: installer379.apk

Size: 13.75MB

MD5: 97faf5a650f9208763df6fead1c60dcf

SHA1: 30a92bf7b674bdff3e62bbd0ae028fad87c335a6

SHA256: c75eb648ed5e71793ae27bdcce3ebaecdc093bdcf53370134dedb0ba09b6f12e

i APP INFORMATION

App Name: MTG Familiar

Package Name: com.gelakinetic.mtgfam

Main Activity: com.gelakinetic.mtgfam.FamiliarActivity

Target SDK: 29 Min SDK: 21 Max SDK:

Android Version Name: 3.6.6.dbg.3

Android Version Code: 75

EE APP COMPONENTS

Activities: 2 Services: 2 Receivers: 3 Providers: 2

Exported Activities: 1 Exported Services: 0 Exported Receivers: 2 Exported Providers: 0



APK is signed v1 signature: True v2 signature: False v3 signature: False

Found 1 unique certificates

Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2012-08-29 14:23:17+00:00 Valid To: 2040-01-15 14:23:17+00:00

Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Serial Number: 0x503e25d5 Hash Algorithm: sha1

md5: e6597ecf05cc58aeeb3653013228c692

sha1: 73fcb682dcae55018f560a303d7e3006b21d45ed

sha256: b42fa6a3fb4bae0dc014633bc7d7fc95d2c2640cb135e257cd71924149f8d64b

sha512: e8461ab8a92051b2bdd5f05631fd837a75b7059cbb25b8b8b5c24e09bd640fb7bded0a81f8e6e41778c8645ccf0b43027d56255b48eaa86fbcc007fc404cd6d4

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

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	high	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.

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.



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

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.gelakinetic.mtgfam.FamiliarActivity	Schemes: card://, http://, https://, Hosts: multiverseid, gatherer.wizards.com, www.wizards.com, Path Prefixes: /, /Pages/Card, /Pages/Search/Default.aspx?name=, /magic/autocard.asp?name=,

△ NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

Q MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]		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.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Activity (com.gelakinetic.mtgfam.MtgAppWidgetConfigure) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
4	Broadcast Receiver (com.gelakinetic.mtgfam.helpers.MTGFamiliarAppWidgetProviderDark) 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.
5	Broadcast Receiver (com.gelakinetic.mtgfam.helpers.MTGFamiliarAppWidgetProviderLight) 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.



NO	ISSUE	SEVERITY	STANDARDS	FILES
				me/zhanghai/android/materialprogressbar/ MaterialProgressBar.java com/bumptech/glide/load/resource/gif/GifD rawableEncoder.java com/bumptech/glide/load/resource/gif/Strea mGifDecoder.java com/bumptech/glide/load/engine/cache/Dis kLruCacheWrapper.java com/codetroopers/betterpickers/expirationp icker/ExpirationPickerBuilder.java com/bumptech/glide/load/resource/bitmap/ BitmapImageDecoderResourceDecoder.java com/bumptech/glide/request/SingleRequest. java com/gelakinetic/mtgfam/helpers/LookupAllP ricesTest.java com/gelakinetic/mtgfam/helpers/LookupAllP ricesTest.java com/bumptech/glide/load/engine/executor/ RuntimeCompat.java com/codetroopers/betterpickers/radialtimep icker/CircleView.java com/bumptech/glide/load/resource/bitmap/ TransformationUtils.java com/bumptech/glide/manager/DefaultConne ctivityMonitorFactory.java com/bumptech/glide/load/resource/ImageD ecoderResourceDecoder.java com/bumptech/glide/load/resource/gif/Byte BufferGifDecoder.java com/bumptech/glide/load/resource/gif/Byte BufferGifDecoder.java com/codetroopers/betterpickers/calendardat epicker/CalendarDatePickerDialogFragment.j ava me/zhanghai/android/materialprogressbar/B aseProgressLayerDrawable.java com/bumptech/glide/load/model/ResourceL oader.java

				com/bamptecn/giide/load/engine/Decodejo
NO	ISSUE	SEVERITY	STANDARDS	င်းမျှန်နှင့် com/bumptech/glide/util/pool/FactoryPools.
				java com/bumptech/glide/load/resource/bitmap/ DefaultImageHeaderParser.java com/tokenautocomplete/TokenCompleteTex tView.java com/codetroopers/betterpickers/timezonepi cker/TimeZoneInfo.java com/bumptech/glide/load/data/AssetPathFet cher.java com/bumptech/glide/load/engine/GlideExce ption.java com/codetroopers/betterpickers/timezonepi cker/TimeZoneFilterTypeAdapter.java com/codetroopers/betterpickers/radialtimep icker/RadialTextsView.java com/codetroopers/betterpickers/calendardat epicker/DayPickerView.java com/bumptech/glide/Glide.java com/afollestad/materialdialogs/internal/MD TintHelper.java com/bumptech/glide/module/ManifestParse r.java com/codetroopers/betterpickers/timezonepi cker/TimeZonePickerUtils.java com/bumptech/glide/load/engine/Engine.jav a com/bumptech/glide/load/engine/Engine.jav a com/bumptech/glide/manager/RequestMana gerRetriever.java com/codetroopers/betterpickers/recurrence picker/EventRecurrence.java com/bumptech/glide/load/data/mediastore/ ThumbFetcher.java com/codetroopers/betterpickers/hmspicker/ HmsPickerBuilder.java
	The Ann less information Counti		CWE: CWE-532: Insertion of Sensitive	com/bumptech/glide/manager/SupportRequ estManagerFragment.java com/bumptech/glide/load/resource/bitmap/
1	The App logs information. Sensitive	info	Information into Log File	Downsampler.java

,	information should never be logged.	T	OWASP MASVS: MSTG-STORAGE-3	com/bumptech/glide/glfdecoder/StandardGlf
NO	ISSUE	SEVERITY	STANDARDS	Preceder.java
				com/bumptech/glide/load/data/LocalUriFetc
				her.java
I	1	,		com/bumptech/glide/load/resource/bitmap/
ı	1	,		HardwareConfigState.java
ı	1			com/codetroopers/betterpickers/timezonepi
ı	1			cker/TimeZoneData.java
I	1			com/codetroopers/betterpickers/radialtimep
I	1			icker/RadialPickerLayout.java
I	1	7		com/bumptech/glide/manager/DefaultConne
I	1			ctivityMonitor.java
ı	1	,		com/codetroopers/betterpickers/radialtimep
I	1			icker/AmPmCirclesView.java
ı	1			com/codetroopers/betterpickers/radialtimep
ı	1			icker/RadialTimePickerDialogFragment.java
ı	1			com/codetroopers/betterpickers/radialtimep
ı	1			icker/RadialSelectorView.java
I	1			com/bumptech/glide/load/resource/bitmap/
l	1			VideoDecoder.java
J	1			com/bumptech/glide/load/data/mediastore/
J	1			ThumbnailStreamOpener.java
J	1			com/bumptech/glide/request/target/ViewTar
J	1			get.java
J	1			com/bumptech/glide/load/resource/bitmap/
J	1			DrawableToBitmapConverter.java
J	1			com/afollestad/materialdialogs/MaterialDial
1	1	7		og.java
ı	1			com/bumptech/glide/GeneratedAppGlideMo
ı	1	,		duleImpl.java
ı	1	,		com/github/machinarius/preferencefragmen
ı	1	,		t/PreferenceManagerCompat.java
ı	1	,		com/bumptech/glide/load/resource/bitmap/
1	1			BitmapEncoder.java
1	1	7		
1	1			com/bumptech/glide/load/engine/executor/ GlideExecutor.java
1	1			3
1	1			com/bumptech/glide/load/model/StreamEnc
1	1			oder.java
ı	1			com/bumptech/glide/manager/RequestTrack
ı	1	,		er.java
1				com/bumptech/glide/request/target/Custom

NO	ISSUE	SEVERITY	STANDARDS	ViewTarget.java FormFSumptech/glide/signature/ApplicationV
				ersionSignature.java
		'		com/codetroopers/betterpickers/timepicker/
		'		TimePickerBuilder.java
		'		com/bumptech/glide/gifdecoder/GifHeaderP
		'		arser.java
				com/bumptech/glide/load/engine/prefill/Bit
		'		mapPreFillRunner.java
				com/bumptech/glide/load/engine/DecodePa
				th.java
		'		com/bumptech/glide/load/data/HttpUrlFetch
		'		er.java
		'		com/bumptech/glide/load/engine/cache/Me
				morySizeCalculator.java
				com/bumptech/glide/load/engine/bitmap_re
				cycle/LruArrayPool.java
				com/nineoldandroids/animation/PropertyVal
		'		uesHolder.java
		'		com/codetroopers/betterpickers/datepicker/
		'		DatePickerBuilder.java
		'		com/bumptech/glide/load/engine/bitmap_re
				cycle/LruBitmapPool.java
		'		com/bumptech/glide/load/engine/SourceGe
				nerator.java
		'		com/codetroopers/betterpickers/recurrence
		'		picker/RecurrencePickerDialogFragment.java
				com/bumptech/glide/manager/RequestMana
		'		gerFragment.java
		'		com/bumptech/glide/load/model/ByteBuffer
				Encoder.java
		'		com/codetroopers/betterpickers/numberpic
		'		ker/NumberPickerBuilder.java
				com/bumptech/glide/load/model/ByteBuffer
		'		FileLoader.java
		'		com/bumptech/glide/load/model/FileLoader
				.java
				,
		'		com/gelakinetic/mtgfam/fragments/LifeCoun
				terFragment.java
		'		terragmentjava

NO ISSUE	SEVERITY	STANDARDS	org/jsoup/helper/W3CDom.java Fold Egelakinetic/mtgfam/fragments/dialo LcPlayerDialogFragment.java
Files may contain hardcoded sensitive information like usernan passwords, keys etc.	nes, warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/gelakinetic/mtgfam/helpers/tcgp/Tcpi.java com/gelakinetic/mtgfam/fragments/dialoramiliarDialogFragment.java com/codetroopers/betterpickers/datepicDatePickerDialogFragment.java com/bumptech/glide/load/engine/Engineource.java com/bumptech/glide/load/Option.java com/gelakinetic/mtgfam/fragments/Rulegment.java com/bumptech/glide/manager/RequestMgerRetriever.java com/codetroopers/betterpickers/timepicTimePickerDialogFragment.java com/bumptech/glide/load/engine/ResouacheKey.java com/gelakinetic/mtgfam/fragments/dialoractivex/internal/schedulers/SchedulolFactory.java com/gelakinetic/mtgfam/fragments/GathgsFragment.java com/codetroopers/betterpickers/numbeker/NumberPickerDialogFragment.java com/codetroopers/betterpickers/numbeker/numberPickerDialogFragment.java com/gelakinetic/mtgfam/fragments/SearewFragment.java com/gelakinetic/mtgfam/fragments/DecknterFragment.java com/gelakinetic/mtgfam/fragments/DecknterFragment.java com/gelakinetic/mtgfam/fragments/DecknterFragment.java com/gelakinetic/mtgfam/fragments/DecknterFragment.java com/codetroopers/betterpickers/hmspichmsPickerDialogFragment.java com/codetroopers/betterpickers/expiraticker/ExpirationPickerDialogFragment.java com/gelakinetic/mtgfam/fragments/dialoracm/gelakinetic/mtgfam/fragments/dialora

NO	ISSUE	SEVERITY	STANDARDS	com/nytimes/android/external/store3/base/i
				ResultListDialogFragment.java
3	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/gelakinetic/mtgfam/helpers/FamiliarLo gger.java com/gelakinetic/mtgfam/fragments/CardVie wFragment.java com/gelakinetic/mtgfam/helpers/ZipUtils.jav a com/gelakinetic/mtgfam/helpers/updaters/D bUpdaterService.java
4	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/gelakinetic/mtgfam/fragments/dialogs/ CardViewDialogFragment.java com/gelakinetic/mtgfam/fragments/CardVie wFragment.java com/gelakinetic/mtgfam/fragments/RulesFra gment.java
5	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/gelakinetic/mtgfam/helpers/database/D atabaseManager.java com/gelakinetic/mtgfam/helpers/database/D atabaseHelper.java com/gelakinetic/mtgfam/helpers/database/C ardDbAdapter.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/afollestad/materialdialogs/BuildConfig.j ava
7	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/gelakinetic/mtgfam/fragments/DiceFragment.java com/gelakinetic/mtgfam/fragments/ResultListFragment.java com/gelakinetic/mtgfam/fragments/MoJhoStoFragment.java org/jsoup/helper/DataUtil.java

■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application use no DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
10	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1/SHA-256/SHA-384/SHA-512 and message digest sizes 160/256/384/512 bits.
11	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
12	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
robobunny.com	ok	IP: 71.158.88.45 Country: United States of America Region: North Carolina City: Raleigh Latitude: 35.772099 Longitude: -78.638611 View: Google Map

DOMAIN	STATUS	GEOLOCATION
creativecommons.org	ok	IP: 172.67.34.140 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
api.tcgplayer.com	ok	IP: 3.212.121.4 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
www.wizards.com	ok	IP: 23.222.47.191 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
gatherer.wizards.com	ok	IP: 199.33.216.39 Country: United States of America Region: Washington City: Renton Latitude: 47.481884 Longitude: -122.196617 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.bluewizard.net	ok	IP: 98.191.209.200 Country: United States of America Region: Virginia City: Arlington Latitude: 38.881008 Longitude: -77.104279 View: Google Map
www.gnu.org	ok	IP: 209.51.188.116 Country: United States of America Region: Massachusetts City: Boston Latitude: 42.358429 Longitude: -71.059769 View: Google Map
raw.githubusercontent.com	ok	IP: 185.199.109.133 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map
schemas.android.com	ok	No Geolocation information available.
github.com	ok	IP: 140.82.121.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
api.scryfall.com	ok	IP: 172.67.73.77 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
www.reddit.com	ok	IP: 199.232.149.140 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
tcgplayer.com	ok	IP: 192,230.74.118 Country: United States of America Region: California City: Redwood City Latitude: 37.532440 Longitude: -122.248833 View: Google Map

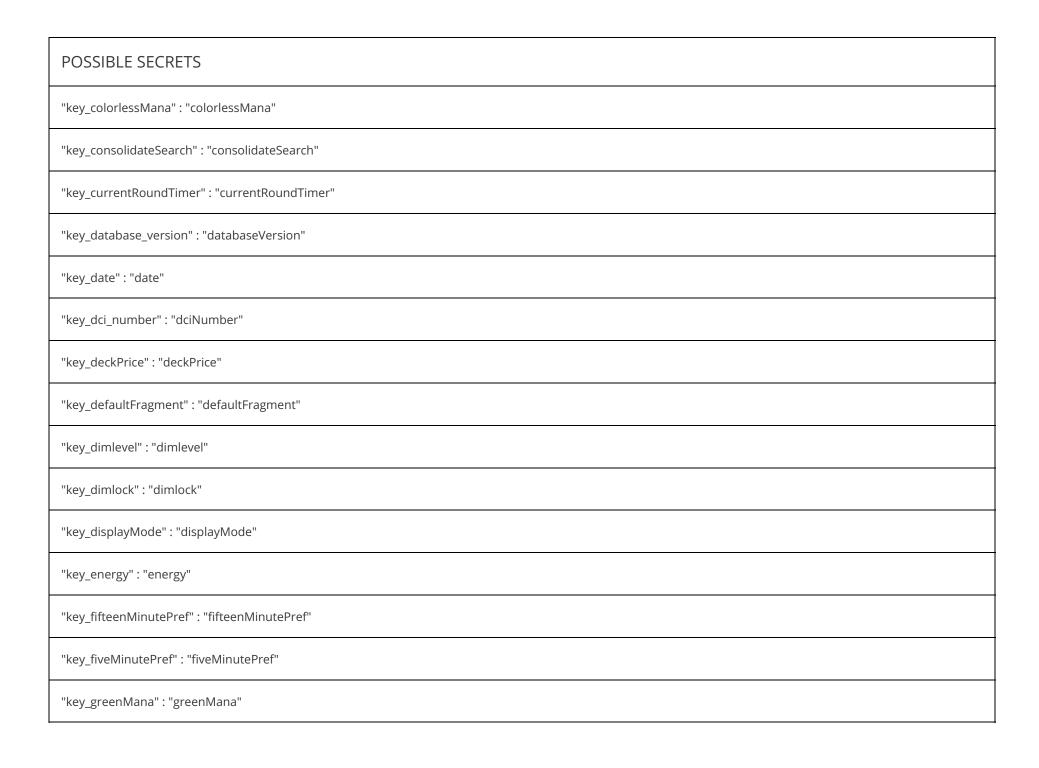
EMAILS

EMAIL	FILE
mtg.familiar@gmail.com	com/gelakinetic/mtgfam/helpers/FamiliarLogger.java

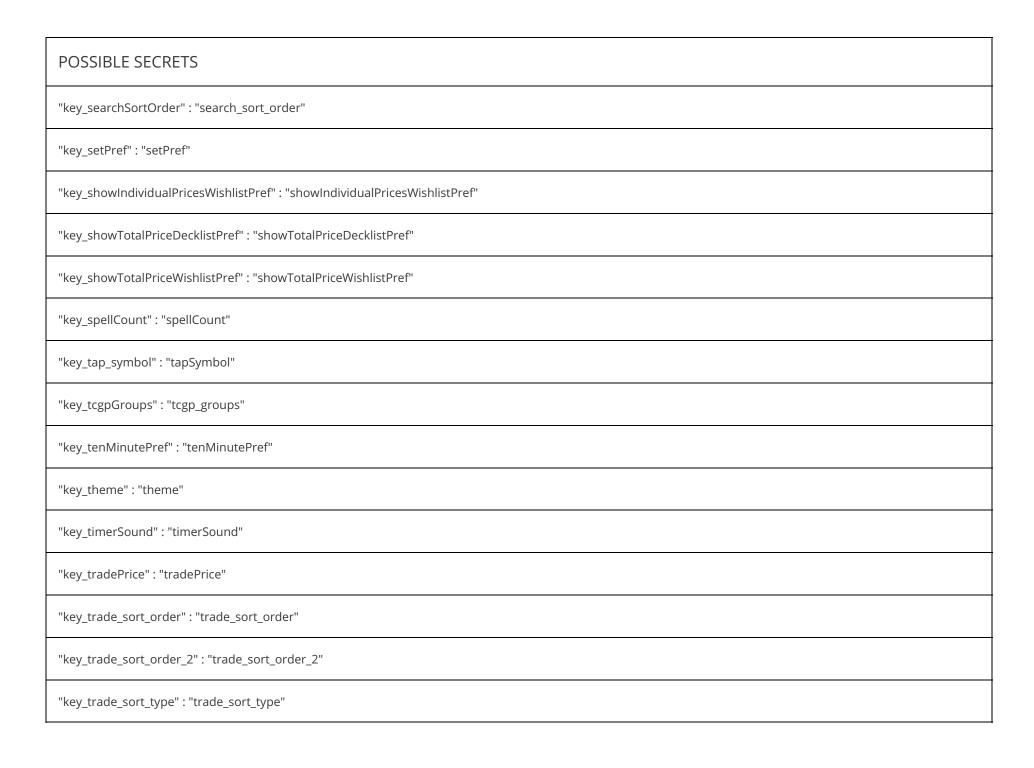
EMAIL	FILE
mtg.familiar@gmail.com	Android String Resource

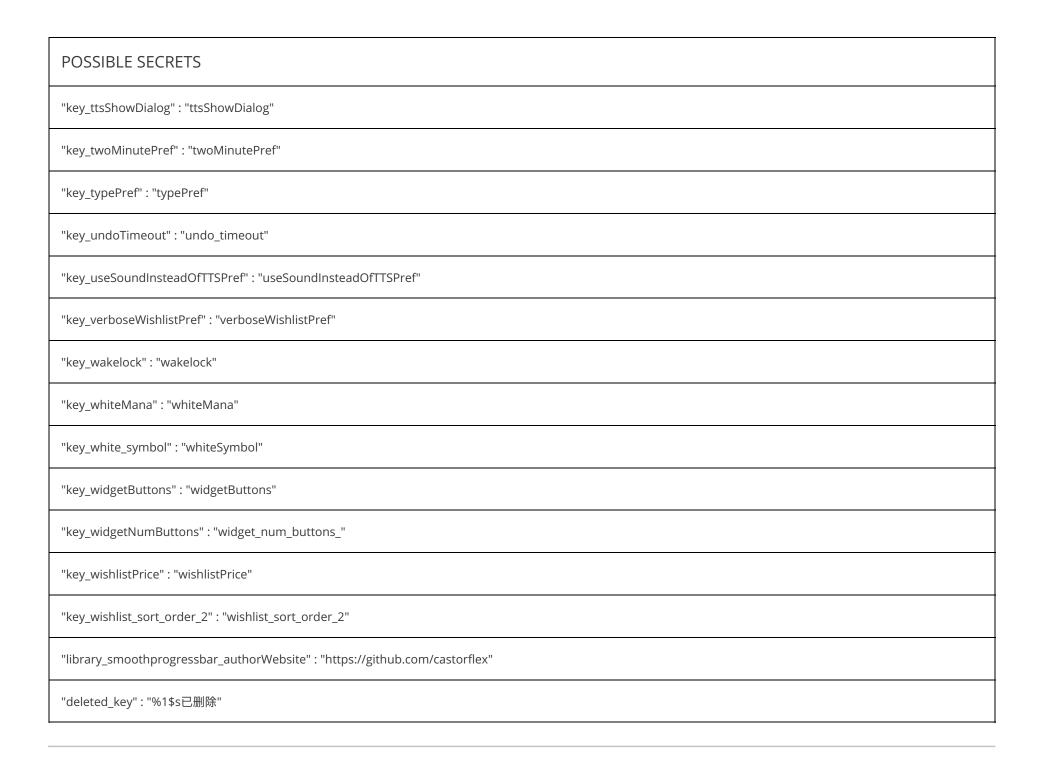
HARDCODED SECRETS

POSSIBLE SECRETS
"key_LastDecklistLoaded" : "last_decklist_loaded"
"key_LastTradeLoaded" : "last_trade_loaded"
"key_SearchCriteria" : "search_criteria"
"key_SearchCriteriaPerm" : "search_criteria_permanent"
"key_TcgpToken" : "tcgp_token"
"key_TcgpTokenExpirationDate" : "tcgp_token_expiration_date"
"key_abilityPref" : "abilityPref"
"key_blackMana" : "blackMana"
"key_blueMana" : "blueMana"
"key_bounceDrawer" : "bounceDrawer"
"key_cardlanguage" : "cardlanguage"









Report Generated by - MobSF v3.5.2 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.

© 2022 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.