ANDROID STATIC ANALYSIS REPORT

DixMax (2.1.9)

File Name:	dixmax-v2.1.9-Android.apk
Package Name:	es.shufflex.dixmax.android
Scan Date:	Oct. 25, 2023, 11:59 a.m.
App Security Score:	35/100 (HIGH RISK)
Grade:	C
Trackers Detection:	3/428

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
9	17	1	1	2

FILE INFORMATION

File Name: dixmax-v2.1.9-Android.apk
Size: 11.18MB
MD5: 0d1694a034bdcfbe0672f456ef482601
SHA1: 44fa71fa5801f4a2e9b3c00f7af3d5b3d3d55058
SHA256: 86cbb3db594dd0a571db23c74badbe1dd7bc8d4ed84606f3dd0a1577f524704e

APP INFORMATION

App Name: DixMax
Package Name: es.shufflex.dixmax.android
Main Activity: es.shufflex.dixmax.android.activities.CastControl
Target SDK: 33
Min SDK: 21
Max SDK:
Android Version Name: 2.1.9

Android Version Code: 170

APP COMPONENTS

Activities: 36
Services: 11
Receivers: 5
Providers: 4
Exported Activities: 6
Exported Services: 1
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=ES, ST=Valencia, L=Alicante, O=Shufflex, OU=Shufflex, CN=Shufflex
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-10-21 23:36:58+00:00
Valid To: 2043-10-15 23:36:58+00:00
Issuer: C=ES, ST=Valencia, L=Alicante, O=Shufflex, OU=Shufflex, CN=Shufflex
Serial Number: 0x692081a3
Hash Algorithm: sha256
md5: 5ca0ea01767893b4fe886483bc8fdab0
sha1: 28d5d645dbd5b36a9e76a49d9be036f1579f79f5
sha256: 169fa95138b28a152914a608a6c585fa11819c96e24fe60ab90deb2833132807
sha512: 7f5984b3dec06366e1fb40b1cab08aec8013708259960cc1bef8c573fac61aa2ec52b27f0560fbb7335428f5d2f8e6c10f1cd6ad3743d4b82e8ac3dde9a5433f
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: c12489d810d0686251c5ad2d0c5bdadc0b87f91eb8b43ae8bf20f34ac3e7e3a8
Found 1 unique certificates
```

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
es.shufflex.dixmax.android.ACCESS_VIDEO_DATA	unknown	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.CHANGE_WIFI_MULTICAST_STATE	normal	allow Wi-Fi Multicast reception	Allows an application to receive packets not directly addressed to your device. This can be useful when discovering services offered nearby. It uses more power than the non-multicast mode.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
com.android.launcher.permission.INSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
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.QUERY_ALL_PACKAGES	normal		Allows query of any normal app on the device, regardless of manifest declarations.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	dangerous		Allows an app to post notifications
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	unknown	Unknown permission	Unknown permission from android reference
es.shufflex.dixmax.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference

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.HARDWARE check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
es.shufflex.dixmax.android.Main	Schemes: http://, https://, moviesv1://, seriesv1://, moviesv2://, seriesv2://, invite://, Hosts: *dixmax.cc, *stream.dixmax.cc, *dixmax.co, *stream.dixmax.co, Path Prefixes: /movie/, /serie/, /v2/movie/, /v2/serie/, /invite/,
es.shufflex.dixmax.android.activities.Pure	Schemes: http://, https://, content://, file://, Mime Types: video/*,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.

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: **8** | WARNING: **4** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=21]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 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	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
4	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.
5	Activity (es.shufflex.dixmax.android.Main) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Activity (es.shufflex.dixmax.android.activities.Pure) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Broadcast Receiver (es.shufflex.dixmax.android.services.DownloaderReceiver) is not Protected. [android:exported=true]	high	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	Activity (es.shufflex.dixmax.android.activities.tv.activities.LoginActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Activity (es.shufflex.dixmax.android.activities.tv.activities.LeanbackActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Activity (es.shufflex.dixmax.android.activities.tv.activities.VideoDetailsActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Activity (es.shufflex.dixmax.android.activities.tv.activities.PlayerActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
12	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.
13	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.

CODE ANALYSIS

HIGH: **0** | WARNING: **9** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a2/d.java b0/c.java b1/b.java c1/g0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				c1/q0.java c2/i.java c3/h.java c3/o.java c4/b.java com/bumptech/glide/b.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java com/github/javiersantos/licensing/APKExpansionPolicy.java com/github/javiersantos/licensing/LibraryChecker.java com/github/javiersantos/licensing/LibraryValidator.java com/github/javiersantos/licensing/ServerManagedPolicy.java com/github/javiersantos/licensing/util/URIQueryDecoder.java com/github/javiersantos/piracychecker/PiracyChecker$start$1$doNotAllow$1$1.java com/journeyapps/barcodescanner/a.java com/journeyapps/barcodescanner/e.java com/unity3d/ads/UnityAds.java com/unity3d/ads/metadata/InAppPurchaseMetaData.java com/unity3d/ads/metadata/MetaData.java com/unity3d/services/UnityServices.java com/unity3d/services/ads/UnityAdsImplementation.java com/unity3d/services/ads/adunit/AdUnitActivity.java com/unity3d/services/ads/adunit/VideoPlayerHandler.java com/unity3d/services/ads/api/AdUnit.java com/unity3d/services/ads/api/VideoPlayer.java com/unity3d/services/ads/api/WebPlayer.java com/unity3d/services/ads/configuration/A

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/unity3d/services/ads/configuration/AdsModuleConfiguration.java com/unity3d/services/ads/load/LoadModule.java com/unity3d/services/ads/video/VideoPlayerView.java com/unity3d/services/ads/webplayer/WebPlayerView.java com/unity3d/services/ar/ARUtils.java com/unity3d/services/ar/view/ARView.java com/unity3d/services/ar/view/GLSurfaceView.java com/unity3d/services/ar/view/ShaderLoader.java com/unity3d/services/banners/BannerView.java com/unity3d/services/banners/UnityBanners.java com/unity3d/services/core/api/Cache.java com/unity3d/services/core/api/DeviceInfo.java com/unity3d/services/core/api/Intent.java com/unity3d/services/core/api/Request.java com/unity3d/services/core/api/Sdk.java com/unity3d/services/core/broadcast/BroadcastEventReceiver.java com/unity3d/services/core/cache/CacheDirectory.java com/unity3d/services/core/cache/CacheThread.java com/unity3d/services/core/cache/CacheThreadHandler.java com/unity3d/services/core/configuration/Configuration.java com/unity3d/services/core/configuration/EnvironmentCheck.java com/unity3d/services/core/configuration/InitializationNotificationCenter.java com/unity3d/services/core/configuration/I

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	nitializeThread.java com/unity3d/services/core/connectivity/ConnectivityMonitor.java com/unity3d/services/core/device/AdvertisingId.java com/unity3d/services/core/device/Device.java com/unity3d/services/core/device/OpenAdvertisingId.java com/unity3d/services/core/device/Storage.java com/unity3d/services/core/log/DeviceLog.java com/unity3d/services/core/misc/JsonStorage.java com/unity3d/services/core/misc/Utilities.java com/unity3d/services/core/misc/ViewUtilities.java com/unity3d/services/core/preferences/AndroidPreferences.java com/unity3d/services/core/properties/ClientProperties.java com/unity3d/services/core/properties/SdkProperties.java com/unity3d/services/core/request/SDKMetrics.java com/unity3d/services/core/request/WebRequest.java com/unity3d/services/core/request/WebRequestRunnable.java com/unity3d/services/core/request/WebRequestThread.java com/unity3d/services/core/sensorinfo/SensorInfoListener.java com/unity3d/services/core/webview/WebView.java com/unity3d/services/core/webview/WebViewApp.java com/unity3d/services/core/webview/bridge/Invocation.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/unity3d/services/core/webview/bridge/NativeCallback.java com/unity3d/services/core/webview/bridge/WebViewBridge.java com/unity3d/services/core/webview/bridge/WebViewBridgeInterface.java com/unity3d/services/core/webview/bridge/WebViewCallback.java com/unity3d/services/monetization/UnityMonetization.java com/unity3d/services/monetization/core/utilities/JSONUtilities.java com/unity3d/services/monetization/placementcontent/core/PlacementContent.java com/unity3d/services/purchasing/core/TransactionDetailsUtilities.java com/unity3d/services/purchasing/core/TransactionErrorDetailsUtilities.java com/unity3d/services/purchasing/core/api/CustomPurchasing.java com/unity3d/services/store/StoreBilling.java d2/h.java es/shufflex/dixmax/android/activities/tv/activities/PlayerActivity.java g1/u.java g5/d.java h0/c.java h2/a.java j1/d.java j1/e.java k3/b0.java k3/q.java k3/u.java l1/c.java l1/e.java m1/h.java m1/i.java m1/k.java m1/q.java m1/z.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				m3/v.java m3/z1.java n1/i.java n1/k.java o/d.java o0/a.java o1/e.java o1/i.java o3/b.java p1/a.java p2/j.java q1/c.java q1/d.java q1/f.java q1/s.java q1/t.java q2/a.java q2/c.java q2/g.java q2/h.java q2/l.java q2/n.java q2/q.java q5/e.java r0/c.java s0/a.java s1/l.java t/a.java t1/c.java t1/e.java t1/g0.java t1/j.java t1/q.java t1/r.java t1/u.java u0/d1.java u0/j0.java u0/v.java u0/z0.java v0/a.java v0/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				x1/a.java x1/d.java x1/j.java y/f.java y2/x.java z1/f.java z1/o.java z1/p.java z1/r.java z1/s.java z1/v.java
2	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/unity3d/services/core/request/SDKMetrics.java es/shufflex/dixmax/android/activities/MddImporter.java m3/n.java m3/o.java m3/s2.java m3/x2.java u4/a.java u4/b.java v4/a.java w5/b.java
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/unity3d/ads/metadata/InAppPurchaseMetaData.java k1/g.java m1/d.java m1/p.java m1/x.java
4	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	com/journeyapps/barcodescanner/e.java v0/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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/github/javiersantos/piracychecker/utils/LibraryUtilsKt.java com/unity3d/services/core/cache/CacheDirectory.java f3/m0.java m3/b2.java m3/l.java m3/v.java m3/z1.java y2/q0.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	p5/f.java p5/g.java p5/l.java p5/m.java
7	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	c4/c.java l3/p.java x3/a.java
8	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	i3/v.java p3/b.java
9	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	com/github/javiersantos/licensing/LibraryValidator.java com/unity3d/services/core/device/Device.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/unity3d/services/ads/webplayer/WebPlayerView.java com/unity3d/services/core/webview/WebView.java
11	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	m3/s2.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION
config.unityads.unitychina.cn	IP: 119.167.231.221 Country: China Region: Shandong City: Qingdao

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
journeyapps.com	ok	**IP:** 18.67.240.90 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
videobin.co	ok	No Geolocation information available.
purl.org	ok	**IP:** 207.241.239.242 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.781734 **Longitude:** -122.459435 **View:** Google Map
vidcloud.ru	ok	**IP:** 185.53.177.50 **Country:** Germany **Region:** Bayern **City:** Munich **Latitude:** 48.137428 **Longitude:** 11.575490 **View:** Google Map
uqload.com	ok	**IP:** 104.26.0.58 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ajax.googleapis.com	ok	**IP:** 142.250.184.10 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.t	ok	No Geolocation information available.
www.gstatic.com	ok	**IP:** 216.58.215.163 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
twitter.com	ok	**IP:** 104.244.42.193 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
uptostream.com	ok	**IP:** 104.26.11.35 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 142.250.201.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
suzihaza.com	ok	**IP:** 104.21.54.34 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
dixmax.info	ok	No Geolocation information available.
storage.googleapis.com	ok	**IP:** 142.250.185.27 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 216.58.215.132 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.veoh.com	ok	**IP:** 35.83.189.26 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
vjs.zencdn.net	ok	**IP:** 151.101.2.217 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
image.tmdb.org	ok	**IP:** 108.157.109.5 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
maxcdn.bootstrapcdn.com	ok	**IP:** 104.18.10.207 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dixmax-270f5.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
powvibeo.me	ok	**IP:** 75.2.18.233 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
goole.es	ok	**IP:** 185.53.178.50 **Country:** Germany **Region:** Bayern **City:** Munich **Latitude:** 48.137428 **Longitude:** 11.575490 **View:** Google Map
www.google.es	ok	**IP:** 142.250.200.131 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
config.unityads.unity3d.com	ok	**IP:** 212.230.153.81 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **View:** Google Map
www.mp4upload.com	ok	**IP:** 188.114.96.5 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **View:** Google Map
dixmax.co	ok	**IP:** 188.114.97.5 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **View:** Google Map
odistream.com	ok	No Geolocation information available.
schemas.xmlsoap.org	ok	**IP:** 13.107.246.43 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
config.unityads.unitychina.cn	ok	**IP:** 119.167.231.221 **Country:** China **Region:** Shandong **City:** Qingdao **Latitude:** 36.098610 **Longitude:** 120.371941 **View:** Google Map
embedsb.com	ok	**IP:** 199.59.243.225 **Country:** United States of America **Region:** Florida **City:** Tampa **Latitude:** 27.943518 **Longitude:** -82.510269 **View:** Google Map
pvpn.asizesoft.com	ok	**IP:** 91.195.240.13 **Country:** Germany **Region:** Nordrhein-Westfalen **City:** Koeln **Latitude:** 50.933331 **Longitude:** 6.950000 **View:** Google Map
www.google-analytics.com	ok	**IP:** 142.250.184.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
upstream.to	ok	**IP:** 185.178.208.135 **Country:** Russian Federation **Region:** Rostovskaya oblast' **City:** Rostov-na-Donu **Latitude:** 47.235630 **Longitude:** 39.712189 **View:** Google Map
jetload.net	ok	**IP:** 162.210.195.111 **Country:** United States of America **Region:** District of Columbia **City:** Washington **Latitude:** 38.895111 **Longitude:** -77.036369 **View:** Google Map
vtube.to	ok	**IP:** 185.113.8.162 **Country:** Turkey **Region:** Istanbul **City:** Istanbul **Latitude:** 41.013840 **Longitude:** 28.949659 **View:** Google Map
vidfast.co	ok	**IP:** 67.225.218.6 **Country:** United States of America **Region:** Michigan **City:** Lansing **Latitude:** 42.733280 **Longitude:** -84.637764 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
pvp.asizesoft.com	ok	**IP:** 91.195.240.13 **Country:** Germany **Region:** Nordrhein-Westfalen **City:** Koeln **Latitude:** 50.933331 **Longitude:** 6.950000 **View:** Google Map
firebasestorage.googleapis.com	ok	**IP:** 142.250.200.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.themoviedb.org	ok	**IP:** 18.154.48.38 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
jawcloud.co	ok	**IP:** 104.21.95.240 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
admob.com	ok	**IP:** 108.177.15.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
cdnjs.cloudflare.com	ok	**IP:** 104.17.25.14 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
t.me	ok	**IP:** 149.154.167.99 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Lowestoft **Latitude:** 52.475201 **Longitude:** 1.751590 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.googleapis.com	ok	**IP:** 142.250.178.170 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
dixmax.cc	ok	**IP:** 188.114.97.5 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **View:** Google Map
cloudvideo.tv	ok	**IP:** 188.114.96.5 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **View:** Google Map
dood.watch	ok	**IP:** 172.67.154.55 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://dixmax-270f5.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Unity3d Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/121

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "56ce39f256c242a6b45c35c56da979c7"
"firebase_database_url" : "https://dixmax-270f5.firebaseio.com"
"google_api_key" : "AIzaSyA4hJUpm7Hahp3wOn2WvAiZqUMxOIBKz-4"

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyA4hJUpm7Hahp3wOn2WvAiZqUMxOIBKz-4"
"library_piracychecker_authorWebsite" : "https://github.com/javiersantos"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
470fa2b4ae81cd56ecbcda9735803434cec591fa
70d407b2-bcb7-4ab2-933c-665bff5e29e5
Gn5384xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJlSAwiGgFAW/dAiS6JXm
JZR6Spejh4U02d8jOt6vLEHfe/JQGiRRSQQxSfFWpi1MquVdAyjUar5+76PVCmYl
aHR0cHM6Ly9qZXRsb2FkLm5ldDo0NDM
f9173f48-8415-4c57-8402-c18ab4d76f3e
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
a24ff7acd3804c205ff06d45
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
aHR0cHM6Ly92aWRjbG91ZC5ydTo0NDM
3f60cfe5-0d17-4739-b658-6b13566ef126

POSSIBLE SECRETS
e2719d58-a985-b3c9-781a-b030af78d30e
a0614e38-1941-44fb-a3e7-5b1ec894db17
888fdc10-f87a-42d1-9c79-2f7819b3dcf2
9a04f079-9840-4286-ab92-e65be0885f95
0250fe34-81ca-4547-aec1-4ff3f70c2c7e
co=aHR0cHM6Ly9qZXRsb2FkLm5ldDo0NDM
9051ed10-b894-4d4f-9738-20cb50061326
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
co=aHR0cHM6Ly92aWRjbG91ZC5ydTo0NDM
1dccb446-5623-43a0-afc6-340ee8913b50
d4000239-bcf3-45fe-960f-18bb40b51034
9d274926-6765-407b-b1dc-1624b7945d36
4d9ee505-a33a-4234-bbf1-af521474fde6

Report Generated by - MobSF v3.7.9 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.