MOBSF

ANDROID STATIC ANALYSIS REPORT

Dream Girlfriend (1.1.0)

File Name:	Dream Girlfriend_1.1.0_Apkpure.xapk
Package Name:	jp.ne.ambition.googleplay_nizikano2d_glb
Scan Date:	Dec. 4, 2023, 12:20 a.m.
App Security Score:	26/100 (CRITICAL RISK)
Grade:	
Trackers Detection:	6/428

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
13	15	1	0	1

FILE INFORMATION

File Name: Dream Girlfriend_1.1.0_Apkpure.xapk
Size: 15.82MB
MD5: 441cb1ded61be0fb76f9a56e2dca69da
SHA1: 674bb7bc46144c4fff05bb69c8a4d6f83eaed63a
SHA256: 8c9425302f6864895803c98b7b5a4b08a7b141f802e2189646a11b9e719e3d0b

APP INFORMATION

App Name: Dream Girlfriend
Package Name: jp.ne.ambition.googleplay_nizikano2d_glb
Main Activity: jp.ne.ambition.googleplay_nizikano2d_glb.Top
Target SDK: 33
Min SDK: 19
Max SDK:
Android Version Name: 1.1.0

Android Version Code: 64

APP COMPONENTS

Activities: 12
Services: 9
Receivers: 8
Providers: 4
Exported Activities: 2
Exported Services: 2
Exported Receivers: 5
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=jp, CN=Ambition
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-05-27 03:54:54+00:00
Valid To: 2040-05-20 03:54:54+00:00
Issuer: C=jp, CN=Ambition
Serial Number: 0x158df4d8
Hash Algorithm: sha256
md5: 8569df457947d7da651ea62dc8ff41a9
sha1: f56ef397d9507a06eb68e7a08e72810af45756b8
sha256: 861f4d34fe9623963c30e6465ca6c74bfcf96c1977cdd74a8da85607f991fdce
sha512: 1b1715d37350cd3b1b271852bd876dbe13639782a936e7831c9fb7434fa928ab045fc903dbbe863fb7517be64eaa779b7d755f649ea09eebdf07a35fdc8f5d25
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 64b2d4f5f8aa10541955710ca2420ac4cac92c9ef7fd9e148f24a939662acdc2
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.SCHEDULE_EXACT_ALARM	normal		Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.google.android.gms.permission.AD_ID	unknown	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	dangerous		Allows an app to post notifications

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.TAGS check SIM operator check network operator name check ro.kernel.qemu check possible VM check FINDINGS: Compiler DETAILS: r8

<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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
network operator name check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
jp.ne.ambition.googleplay_nizikano2d_glb.Top	Schemes: ambition-nizikano2d-glb-browser://, Hosts: nizikano,
jp.ne.ambition.googleplay_nizikano2d_glb.Nizikano	Schemes: ambition-nizikano2d-glb://, Hosts: main, twitter, ad,
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.jp.ne.ambition.googleplay_nizikano2d_glb,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	amz-aws.jp	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

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: 10 | WARNING: 5 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=19]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	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.
3	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.
4	Launch Mode of activity (jp.ne.ambition.googleplay_nizikano2d_glb.Top) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
5	Launch Mode of activity (jp.ne.ambition.googleplay_nizikano2d_glb.Title) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
6	Launch Mode of activity (jp.ne.ambition.googleplay_nizikano2d_glb.Nizikano) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Activity (jp.ne.ambition.googleplay_nizikano2d_glb.Nizikano) 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.
8	Broadcast Receiver (jp.ne.ambition.googleplay_nizikano2d_glb.PushReceiver) 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.
9	Service (jp.ne.ambition.googleplay_nizikano2d_glb.FcmService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Broadcast Receiver (com.tapjoy.InstallReferrerReceiver) 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.
11	Broadcast Receiver (com.tapjoy.GCMReceiver) 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.
12	Broadcast Receiver (com.tapjoy.TapjoyReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
13	Content Provider (com.facebook.FacebookContentProvider) is not Protected. [android:exported=true]	high	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.
14	Activity (com.facebook.CustomTabActivity) 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.
15	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.
16	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: 1 | WARNING: 8 | INFO: 1 | SECURE: 0 | SUPPRESSED: 0

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	bolts/MeasurementEvent.java com/appsflyer/AFLogger.java com/tapjoy/HmacSignature.java com/tapjoy/TJAdUnitJSBridge.java com/tapjoy/TJCloseButton.java com/tapjoy/TJPlacement.java com/tapjoy/TJPlacementManager.java com/tapjoy/TJSplitWebView.java com/tapjoy/TJWebViewJSInterface.java com/tapjoy/TapjoyAdIdClient.java com/tapjoy/TapjoyAppSettings.java com/tapjoy/TapjoyCache.java com/tapjoy/TapjoyCacheMap.java com/tapjoy/TapjoyCachedAssetData.java com/tapjoy/TapjoyConnectCore.java com/tapjoy/TapjoyGpsHelper.java com/tapjoy/TapjoyLog.java com/tapjoy/TapjoyURLConnection.java com/tapjoy/TapjoyUtil.java com/tapjoy/internal/dn.java com/tapjoy/internal/es.java com/tapjoy/internal/fl.java com/tapjoy/internal/fm.java com/tapjoy/internal/fq.java com/tapjoy/internal/fz.java com/tapjoy/internal/jk.java jp/live2d/ALive2DModel.java jp/live2d/Live2D.java jp/live2d/ModelContext.java jp/live2d/android/b.java jp/live2d/base/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				jp/live2d/base/d.java jp/live2d/graphics/DrawParam.java jp/live2d/motion/Live2DMotion.java jp/live2d/motion/Live2DMotion2.java jp/live2d/motion/MotionQueueManager.java jp/live2d/param/b.java jp/live2d/util/UtDebug.java jp/live2d/util/a.java jp/ne/ambition/googleplay_nizikano2d_glb/ImageGetTask.java jp/ne/ambition/googleplay_nizikano2d_glb/LogUtil.java jp/ne/ambition/googleplay_nizikano2d_glb/Top.java
2	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	com/appsflyer/internal/af.java
3	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/appsflyer/internal/af.java com/tapjoy/internal/ch.java
4	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/tapjoy/TapjoyLog.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	bolts/MeasurementEvent.java com/appsflyer/AppsFlyerProperties.java com/tapjoy/TapjoyConstants.java jp/ne/ambition/googleplay_nizikano2d_glb/Basic.java jp/ne/ambition/googleplay_nizikano2d_glb/Constant.java
6	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/tapjoy/internal/g.java com/tapjoy/internal/gg.java
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	jp/ne/ambition/googleplay_nizikano2d_glb/Top.java
8	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/tapjoy/TapjoyCache.java
9	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	bolts/WebViewAppLinkResolver.java
10	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/tapjoy/internal/hx.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

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
us-nizi2d-app.amz-aws.jp	ok	**IP:** 18.67.17.59 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 142.251.32.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
rpc.tapjoy.com	ok	**IP:** 54.147.102.189 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
smonitorsdk.s	ok	No Geolocation information available.
sapp.s	ok	No Geolocation information available.
dream-girlfriend-23ec4.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ws.tapjoyads.com	ok	**IP:** 3.162.3.94 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
dev.tapjoy.com	ok	**IP:** 54.192.51.10 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.714272 **Longitude:** -74.005966 **View:** Google Map
placements.tapjoy.com	ok	**IP:** 54.172.247.174 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
dev.tapjoy.comfor	ok	No Geolocation information available.
tech.tapjoy.com	ok	**IP:** 54.236.103.17 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 172.217.13.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sregister.s	ok	No Geolocation information available.
connect.tapjoy.com	ok	**IP:** 52.6.186.230 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://dream-girlfriend-23ec4.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Tapjoy		https://reports.exodus-privacy.eu.org/trackers/199

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://dream-girlfriend-23ec4.firebaseio.com"
"google_api_key" : "AIzaSyAs-Xw8RCClcMJUNxkFWDCQ7fTvBkqG21I"
"google_crash_reporting_api_key" : "AIzaSyAs-Xw8RCClcMJUNxkFWDCQ7fTvBkqG21I"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
Fd8OOLu4RKKEBnvX8a2CQAECAXCBnLNZJqgWZtk5zufQhiNdCpQVfC2rB
iVBORw0KGgoAAAANSUhEUgAAAA0AAAANCAYAAABy6+R8AAAAAXNSR0IArs4c6QAAAHtJREFUKBWVkksKwCAMREOh99+3y97GU3iTdp6tRcUoBgbJfEgCmpkF4RA2YVTo+PDbKdzCJXhBeHR8BJMxE71gGah0T/B4hqVqDbvY0QZfrF41ip3d+geZkAO89MMqV4xyTieVAW6Z3tQG6CmP94U319dXfwT+pb9HIDwrxDUcBOiFBQAAAABJRU5ErkJggg==

POSSIBLE SECRETS
9b8f518b086098de3d77736f9458a3d2f6f95a37
eWzIsJF4PExQap9HK6Vlz8DGlgGwoiLCtyOEK0Bfu
iVBORw0KGgoAAAANSUhEUgAAAAgAAAANCAYAAACUwi84AAAAAXNSR0IArs4c6QAAAHlJREFUGBljZsAOBIHCu4FYC5u0GFDwAhD/B+IN6ApkgAI3oJIrgTQrsgJlIOc+VHIukGZCltQGcp5BJScCaUZkSWMg5w1UshlZAsa+A5XcCRNApwmaANKA7IYJQD6KG2Am4vUFTBHecIApQglJrHYBVYLiYhMQnwAAeiYfS1LRd+4AAAAASUVORK5CYII=
iVBORw0KGgoAAAANSUhEUgAAABAAAAAaCAYAAAC+aNwHAAAAAXNSR0IArs4c6QAAAPZJREFUOBFjYCAdWAG1PADiCUDMBMQkAReg6i9A/B+KZ5Ki2w+o+AeSZpAhF4g1IBKo8Dea5utAvjQxBqQCFf1F03wOyBclRnMRmkaQs48CsQAxmuuxaN4DFOMmRnMPFs0bgWLshDSD4hUUNbBogtHLgGIshDSDFCzFonkWUIxgggE5bQMWzX1AMYIAFCi7gRjmXBjdSFAnVMFOLJqLidUM8hvIRooALi80kGIqRYEIs4iiaIQZQlFCghkConuBGBadMJqopIxsSD0WQ4jOTDCDcGVnfpgCYmiKChSYBdiKtGtASaKKNJghFBWqMEMoKtZhhqBULADcM3nkekaNxwAAAABJRU5ErkJggg==
eyJhbGciOiJSUzI1NiIsIng1YyI6WyJNSUlDNlRDQ0FkRUNBU293RFFZSktvWklodmNOQVFFTEJRQXdEekVOTUFzR0ExVUVBd3dFVW05dmREQWVGdzB4TkRFeE1UZ3hOalUwTUROYUZ3MHpOREV4TVRNeE5qVTBNRE5hTUdZeEN6QUpCZ05WQkFZVEFsVlRNUk13RVFZRFZRUUlEQXBEWVd4cFptOXlibWxoTVJZd0ZBWURWUVFIREExTmIzVnVkR0ZwYmlCV2FXVjNNUlF3RWdZRFZRUUtEQXRIYjI5bmJHVWdTVzVqTGpFVU1CSUdBMVVFQXd3TFptOXZMbUpoY2k1amIyMHdnZ0VpTUEwR0NTcUdTSWIzRFFFQkFRVUFBNElCRHdBd2dnRUtBb0lCQVFDekZWS0pPa3FUbXl5ak1IV0JPckxkcFltYzBFY3ZHM01vaGFWK1VKclZySTJTRHlrWThZV1NrVEt6OUJLbUY4SFAvR2pQUERzMzE4NENlajliMVdleXZWQjhSajNndUgzb0wrc0pUM3U5VjJ5NHp5bzV4TzZGV01CWUVRNlg4RGtHbFl0VHA1dGhlWWJSclhORUx1bDRsRitMdEhUQ2FBQU5STWtPbDBORW9MYTZCUmhPRzY4Z0ZmSUF4eDVsVDhSRUU5dXR2UHV5K3JDYUJIbmZIT1BmOHBuMExTdmNlQmlqU0lGb1MzWTVjcmpQVmp5aVBBWlVIV25IVEZBaWxmSG5wTEJsR3hwQ3lsZVBRaE1LclBjZ3ZEb0Q5bmQwTEE2eFlMRjdEUFhYU2E4RkxPK2ZQVjhDTkpDQXNGdXE5UmxmMlR0M1NqTHRXUll1aDVMdWN0UDdBZ01CQUFFd0RRWUpLb1pJaHZjTkFRUxCUUFEZ2dFQkFFc01BQlpsKzhSbGswaHFCa3RzRHVycmk0bkYvMDdDblNCZS96VWJUaVloTXByN1ZSSURsSExvZTVsc2xMaWxmWHp2YXltY01GZUgxdUJ4TndoZjdJTzdXdkl3UWVVSFNWK3JIeU55Z1RUaWVPMEpuOEh3KzRTQ29oSEFkTXZENXVXRXduM0x2K1c0eTdPaGFTYnpsaFZDVkNuRkxWS2ljQmF5VVhIdGRKWEpJQ29rUjQraC9XTk03ZzBpS1RoYWtaT3lmYjhoMXBoeTdUTVRWbFBGS3JjVkRvNW05K0dodFBDNFBOakdMb2s2ci9qeDlDSU9DYXBJcWk4ZlhKRU94S3ZpbFllQVlxZmpXdmh4MDBqdUVVQkhycENROHdUNFRBK0xsSTAyY1J6NXJ4VzRGUUF6MU5kb0c5SFpEWldhK05ORlRaZEFtdFdQSk1MZCs4TDhzbDQ9IiwiTUlJQzhUQ0NBZG1nQXdJQkFnSUpBTU5JMTVIckd5bGtNQTBHQ1NxR1NJYjNEUUVCQ3dVQU1BOHhEVEFMQmdOVkJBTU1CRkp2YjNRd0hoY05NVFF4TVRFNE1UWTFOREF6V2hjTk16UXhNVEV6TVRZMU5EQXpXakFQTVEwd0N3WURWUVFERUFSU2IyOTBNSUlCSWpBTkJna3Foa2lHOXcwQkFRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQXplVU5jNGJTV0hoT1RVKzVNUS9sT21talFXcGZCaStGSnV4dm9lT21Rd2k2ZnJQS0tzYUtLWUdmQ1RQbEtFMGRtckVQOTVibmkvcUw1eEFwUDE3b3JqVWU2S1J0SkF3Rk5JNUVaYWRJZmpiaC9xKzg1QzFDcDJCUzJZbXVaUXpYWkhQNjN5eUJwMDVZY2JNS3dDQkhYYUFnWWJtVFRrKzQrMXBqTnBIUDZZaUYyZ0NQdlNmem9rR3loYnZCcW5QYm5UZEk5dzZmak5CWUFici91Qk9UVTB2SzRrdHpsV2s1bHZzbTUxZTh2c0xTcVdob0hBRHEwQXJpQWVsVTRTSHNTQUNrUlVRU3hXVjBLNWh6VHY0ZWN2Q2JHOWRza2lEQ3dXZyt1VFJTb0FGZVpPaE9OTDAwMHE3VmV5M0RaVGNMbDgvTzROUVZhWll1aUFnVldsV2Nzd0lEQVFBQm8xQXdUakFkQmdOVkhRNEVGZ1FVc2ltbElSRGNKUjBvZll3b004S3dIRk9IK3NJd0h3WURWUjBqQkJnd0ZvQVVzaW1sSVJEY0pSMG9mUjdvTThLd0hGT0grc0l3REFZRFZSMFRCQVV3QXdFQi96QU5CZ2txaGtpRzl3MEJBUXNGQUFPQ0FRRUFXUWw4U21iUW9CVjN0ak9KOHpNbGNOMHhPUHBTU05ieDBnN0VML2RRZ0pwZXQwTWNXNjJSSGxnUUFPS2JTM1BSZW8ybnNSQi9aUnlZRHU0aTEzWkhaOGJNc0dPRVM0QlFwejEzbXRtWGc5UmhzWHFMMGVEWWZCY2pqdGxydVVieGhuQUxwNFZOMXpWZHlXQVBDajBldTNNeHBnTVdjeW41MFFtaUpTai9FcXUvbExodmUvd0t2akc1V2huVjh1UktSdUZiRmN0MERIQUhNblpxRkhjR1M1U28wY1luU2ZLNWZiQlJOZWxHZmxocGJiUHAwVjBhWGlxaW5xRDBZZTNPYVpkRnErMnJQMW9DL2E1L091NExzcFkzYjVvRDlyRU5keTdicTBLZXdQRnRnUHZVa0pySjNUemJpd3ZwZ2haN3pHMjZibko1STd1YzR5MVZ1anFhT0E9PSJdfQ

POSSIBLE SECRETS
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
tgLRb4bjuZVA8xvQ9uHNs8UtpBIOiUcagzvtKyyfCofk5U5sNb54GgVVYxa6p4A1ObdJv1jjlUOnzR8keX5LsAM4Ia7xeqiFh0GER4l0ulVChy
W1zcp5YuPDw8mIQDVCH2uQY7qs2ejdZj5LIgIz4CbQ0wg53rlwE7DDQM6MNUgZLnzNmMSMfFrpE7
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
ApUOURgBBlwkJ55qXdBdD7d2BwSxaopnkdC0UMnAa0djwh6n3D
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
yHTAZeApn5rh6Uzfx06Gv6eHdM34YL
5e8f16062ea3cd2c4a0d547876baa6f38cabf625
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
cc2751449a350f668590264ed76692694a80308a

PLAYSTORE INFORMATION

Title: Dream Girlfriend

Score: 3.7818348 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Simulation **Play Store URL:** jp.ne.ambition.googleplay_nizikano2d_glb

Developer Details: Ambition co., ltd., 4685636909317788836, □□□□□□□□□□3-4-3, http://dreamgirlf.com/, info@us.nizikano-2d.jp,

Release Date: Sep 15, 2015 **Privacy Policy:** Privacy link

Description:

The hit Japanese dress-up simulator Dream Girlfriend is being enjoyed by anime fans all around the world, with millions of downloads worldwide! Choose from a huge range of options to customize your girl just like your favorite characters! Chat, interact and watch her move with detailed emotion with Live2D technology! Features: □ Create up to four cute anime girls at once. □Live2D technology adds emotive motion. □11 different personalities with huge speech variation. □A walk-in closet with over 20 different customizable slots. □Updated regularly with events, campaigns and more. □Romantic interactions and fashion competitions included. Join us on social media! Facebook: https://www.facebook.com/dreamgfENG/ Twitter: https://twitter.com/dreamgfENG

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.