



ANDROID STATIC ANALYSIS REPORT



 Play Games Extension (1.0)

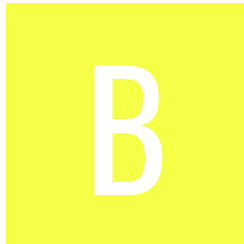
File Name: 3055fc207f21d4140249a3eb3efcdea047dfe005a4c23388ab917ffe3a8515d7.apk

Package Name: com.karabasstudio.nightdescent

Scan Date: April 26, 2025, 8:35 p.m.

App Security Score: 52/100 (MEDIUM RISK)

Grade:



Trackers Detection: 1/432

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
1	6	1	1	1

FILE INFORMATION

File Name: 3055fc207f21d4140249a3eb3efcdea047dfe005a4c23388ab917ffe3a8515d7.apk

Size: 1.58MB

MD5: f64cbd33651a99b08a9168607a2374d1

SHA1: a16bb93ee35e7636e4f824010ddbba975a7db5ed

SHA256: 3055fc207f21d4140249a3eb3efcdea047dfe005a4c23388ab917ffe3a8515d7

APP INFORMATION

App Name: Play Games Extension

Package Name: com.karabasstudio.nightdescent

Main Activity: com.karabasstudio.nightdescent.MainActivity

Target SDK: 26

Min SDK: 14

Max SDK:

Android Version Name: 1.0

Android Version Code: 1

APP COMPONENTS

Activities: 4

Services: 1

Receivers: 1

Providers: 1

Exported Activities: 0

Exported Services: 1

Exported Receivers: 1

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed

v1 signature: True

v2 signature: True

v3 signature: False

v4 signature: False

X.509 Subject: CN=Arif Onur ŞEN

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2019-04-22 18:03:06+00:00

Valid To: 2044-04-15 18:03:06+00:00

Issuer: CN=Arif Onur ŞEN

Serial Number: 0x6b70c5b4

Hash Algorithm: sha256

md5: 1a82d30f1295b0525ff2f23f54672ca9

sha1: 62bc3634d7327ea13ab2baabed276a856d789121

sha256: 00c10f9de39c76177001aa03862bca44dfd5684d9c3e56f589a30690a6fd74d9

sha512: 5266cf89ae10323f7ef7918013e77a9b9714d01aad367e85a97f1934bafba9ff0c279b5eff0bd018f95559ab5f84272fbbb60ca571cf2313670a0330475c6b314

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 5c2814e4d6a0b047c0f91e5ae9b774f5b53ecce7975e255bdce7a4419d486375

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.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.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.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.
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.

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

 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.

Q MANIFEST ANALYSIS

HIGH: 1 | WARNING: 3 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 4.0-4.0.2, [minSdk=14]	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	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	Broadcast Receiver (com.karabasstudio.nightdescent.MainReceiver) 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.karabasstudio.nightdescent.MainService) is not Protected. [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.

</> CODE ANALYSIS

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

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/karabasstudio/nightdescent/MainAdActivity.java com/karabasstudio/nightdescent/MainService.java com/karabasstudio/nightdescent/MainWebService.java
2	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/karabasstudio/nightdescent/RetrofitClient.java

NIAP ANALYSIS v1.3

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

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/karabasstudio/nightdescent/MainService.java com/karabasstudio/nightdescent/MainWebService.java
00036	Get resource file from res/raw directory	reflection	com/karabasstudio/nightdescent/MainService.java
00013	Read file and put it into a stream	file	okio/Okio.java

RULE ID	BEHAVIOUR	LABEL	FILES
00054	Install other APKs from file	reflection	com/karabasstudio/nightdescent/MainWebService.java
00191	Get messages in the SMS inbox	sms	com/karabasstudio/nightdescent/MainWebService.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.REQUEST_INSTALL_PACKAGES, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	0/44	

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312

HARDCODED SECRETS

POSSIBLE SECRETS
PQw299M+gyZAcirIo44nMA1T6aZFSbwBV2vuW7mK5no=
SC+voVwtFTxxanSuPBwO3gUspzEVAamsN8QrPnkhP0Y=
U6RyofmU5fe6F6Q76ZqotRxxCpQcx2ZA3KAikgaYO1E=
7KqrGXdk/af3XqeV7Kdf9Pblbh3C1JbHd2XfO7vMbAGonJ11eSDtjbVaiMZyTrse
wFR9IVBeC3DxjLUHG4VrPvC6sFnF3i6EXAzgF2FV6F/P1tVlXRsZCqzBo3bMqAjwt
Vd8F7XEjcopfPCqlo7UkH81gSF32pH8ICaByQHEDSARI1QZSSarfP6NUtOQ3X7FJ
B3EEABB8EE11C2BE770B684D95219ECB
SqEbpmL0PRd8OMIcAaTW+Qm/eIldjoaBC5+hlpZQMKI=
Oqhihr+ZvNwej7GnFvAZoFFN+/Dv8PoAOgFukKxDQRFkh0v6oq6svnLeRKh0PLMP
z4IUOMEUJjwo87MrwW0oo5MuoOqDlnlQo6iV4pjz2VLab+vfSTsyph6zr+NoPrYU
8yXffwi9xD4yRk9s3bzICsp78O1cQWIN/y7cfZ1O0xQ=
oyXxJz1/0whZ1sjpKwx6gZrLwCk4v4rbcD6dwdNy6Cs=
J+RI1JNo03xly9SRWO99cvEQhgdX6x+RL8PvxYQsPic=
ljgMduD5kKPhK6qoocDB5WikKD/CX1UhLGscwfdkLacCDIfdaQLvcdICLYIVWEY

POSSIBLE SECRETS
258EAFa5-E914-47DA-95CA-C5AB0DC85B11
AlzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
aHR0cDovL2FkbW9iLWdhbWVzLn5eg==
L28yi1GnuU8llvgZA5ti7bBAIAb8V1oFU13C+ZO3hWQ=
8e8MBQUUwetjXHXD+OHa6GoKdEoeWcCKvjd/0LAqmt67vps6BIKdZS4FehPCaFQs
qrGvg6pF9No4qMDhGfUiE0qkqx8DIEl1ObOP4v8z9Vw=
zUtdaly7f7RI0b3U/Ak3WbCr4NUUCFrNIppHHrQ+Up0=
QZZCt2ftWILMiOv/bx0NwH1VFPjOT+QCiqkEm96fZOY=
polTj6KYBt5BdnGUyKVpTqoje9uUrbj0v36XCagBsYjc7oBvjejRtfajj7hby90a
UrT94Dq3ubetC7rQ64nVjqMQ53po9X61geGgrP+ILCU=
ZdvpwpF09ah9qMkbMMBkQbN3G9MUkP5Jgcz6nA07dkM=
lzCo36nc7XBNxigvUEYksuBFsczDyb5Knn+0+OBVmAuGHrrlrxjgxEWtsLNUGdmh
085nDtgvdnF/9q+L3rbTJRP85nBeHpWsnwPQ5NbQuGUMVoHq922oSf9teCh818O7
FngGcM4uMQo5eKR2FwSIMJnWgsaWh19tKknwKd4tbUk=
WFWMehHtsFVdDUEDmR6QBWCVOt7vhsukeVfF7GyA4njfn/HGydHkg9TxbsV2ogHj

POSSIBLE SECRETS
IRjV9vmlQsYenNEwAjnRXRcX4jgQUq/mhLu9dLiWkF0=
93FZcx3TGairtssuo4NaSvmwhnBdBRfmG43cez1s4nHLHJg1A/3UR3k+fui87zal
3K8ELf0l97OojkLZ8w0j1a7PyOLXhiU05fzwfJl+q5R78K5HrzBW+Y6Q9dHwMhs9
XHiP8GJo+im4O4z0srsKg+iMpuUpknn3lyfTXGI6thg=

SCAN LOGS

Timestamp	Event	Error
2025-04-26 20:35:05	Generating Hashes	OK
2025-04-26 20:35:05	Extracting APK	OK
2025-04-26 20:35:05	Unzipping	OK
2025-04-26 20:35:05	Parsing APK with androguard	OK
2025-04-26 20:35:05	Extracting APK features using aapt/aapt2	OK

2025-04-26 20:35:05	Getting Hardcoded Certificates/Keystores	OK
2025-04-26 20:35:06	Parsing AndroidManifest.xml	OK
2025-04-26 20:35:06	Extracting Manifest Data	OK
2025-04-26 20:35:06	Manifest Analysis Started	OK
2025-04-26 20:35:06	Performing Static Analysis on: Play Games Extension (com.karabasstudio.nightdescent)	OK
2025-04-26 20:35:06	Fetching Details from Play Store: com.karabasstudio.nightdescent	OK
2025-04-26 20:35:07	Checking for Malware Permissions	OK
2025-04-26 20:35:07	Fetching icon path	OK
2025-04-26 20:35:07	Library Binary Analysis Started	OK
2025-04-26 20:35:07	Reading Code Signing Certificate	OK

2025-04-26 20:35:07	Running APKiD 2.1.5	OK
2025-04-26 20:35:08	Updating Trackers Database....	OK
2025-04-26 20:35:08	Detecting Trackers	OK
2025-04-26 20:35:08	Decompiling APK to Java with JADX	OK
2025-04-26 20:35:12	Converting DEX to Smali	OK
2025-04-26 20:35:12	Code Analysis Started on - java_source	OK
2025-04-26 20:35:13	Android SBOM Analysis Completed	OK
2025-04-26 20:35:13	Android SAST Completed	OK
2025-04-26 20:35:13	Android API Analysis Started	OK
2025-04-26 20:35:14	Android API Analysis Completed	OK
2025-04-26 20:35:14	Android Permission Mapping Started	OK

2025-04-26 20:35:14	Android Permission Mapping Completed	OK
2025-04-26 20:35:14	Android Behaviour Analysis Started	OK
2025-04-26 20:35:15	Android Behaviour Analysis Completed	OK
2025-04-26 20:35:15	Extracting Emails and URLs from Source Code	OK
2025-04-26 20:35:15	Email and URL Extraction Completed	OK
2025-04-26 20:35:15	Extracting String data from APK	OK
2025-04-26 20:35:15	Extracting String data from Code	OK
2025-04-26 20:35:15	Extracting String values and entropies from Code	OK
2025-04-26 20:35:15	Performing Malware check on extracted domains	OK
2025-04-26 20:35:15	Saving to Database	OK

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.

© 2025 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).