

ANDROID STATIC ANALYSIS REPORT



• Andor's Trail (0.7.11)

File Name:	installer204.apk
Package Name:	com.gpl.rpg.AndorsTrail
Scan Date:	May 30, 2022, 4:03 p.m.
App Security Score:	45/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	ℚ HOTSPOT
2	4	0	1	1

FILE INFORMATION

File Name: installer204.apk

Size: 33.3MB

MD5: 3ef3eaad88a47f4f4843ea497c98c98b

SHA1: 8503b9b947c3bd8a3d2733ec37ad5b925799f003

SHA256: 1015b21ffdced1e08e43ca4da8e926696bbf02c28b22fe6e1965b2aca1714cdd

i APP INFORMATION

App Name: Andor's Trail

Package Name: com.gpl.rpg.AndorsTrail
Main Activity: .activity.StartScreenActivity

Target SDK: 28 Min SDK: 4 Max SDK:

Android Version Name: 0.7.11 Android Version Code: 54

EE APP COMPONENTS

Activities: 17 Services: 0 Receivers: 0 Providers: 0

Exported Activities: O Exported Services: O Exported Receivers: O Exported Providers: O

***** CERTIFICATE INFORMATION

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: 2011-10-02 11:00:04+00:00 Valid To: 2039-02-17 11:00:04+00:00

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

Serial Number: 0x4e884434 Hash Algorithm: sha1

md5: cc0f29e57d558dc11759e702bea7063a

sha1: 3d3b3722ee92eb5cf536f8a74922f999a620d58e

sha256: 3916cb3700f0ab8e79014448d000429b826a59e0b4364b96c94d905a6559d243

sha512: 9e69af56ff5d3218939735ad509ae6a31177e606184ce0b61f6b19608d991bd6c47ac8b07b707acfabc8e9fb7f1ecd873d67d0933ab8e526fcdaead03c6ffee7

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	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.	

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.

命 APKID ANALYSIS

FILE	DETAILS		
------	---------	--	--

FILE	DETAILS				
	FINDINGS	DETAILS			
classes.dex	Compiler	dx (possible dexmerge)			
	Manipulator Found	dexmerge			

△ NETWORK SECURITY

NO SCOPE SEVERITY DESCRIPTION	NO	SCOPE	SEVERITY	DESCRIPTION
-------------------------------	----	-------	----------	-------------

Q MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/gpl/rpg/AndorsTrail/model/map/TMXM apTranslator.java com/gpl/rpg/AndorsTrail/model/map/TMXM apFileParser.java
2	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/gpl/rpg/AndorsTrail/controller/WorldMa pController.java com/gpl/rpg/AndorsTrail/savegames/Savega mes.java com/gpl/rpg/AndorsTrail/AndorsTrailApplicati on.java
3	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/gpl/rpg/AndorsTrail/controller/Constant s.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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 no hardware resources.
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 no network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files 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.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does not encrypt any data in traffic or does not transmit any data 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 not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
andorstrail.com	ok	IP: 184.154.46.111 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
nacred.deviantart.com	ok	IP: 108.156.60.103 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 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
redknight91.deviantart.com	ok	IP: 108.156.60.103 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map

DOMAIN	STATUS	GEOLOCATION
fatboy73.deviantart.com	ok	IP: 108.156.60.103 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
www.tekepon.net	ok	IP: 199.59.243.220 Country: United States of America Region: Florida City: Tampa Latitude: 27.943518 Longitude: -82.510269 View: Google Map
rltiles.sourceforge.net	ok	IP: 204.68.111.100 Country: United States of America Region: California City: San Diego Latitude: 32.799797 Longitude: -117.137047 View: Google Map
telles0808.deviantart.com	ok	IP: 108.156.60.103 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map

DOMAIN	STATUS	GEOLOCATION
discord.gg	ok	IP: 162.159.136.234 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
ayene-chan.deviantart.com	ok	IP: 108.156.60.103 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
forums.wesnoth.org	ok	IP: 95.217.86.148 Country: Finland Region: Uusimaa City: Helsinki Latitude: 60.169521 Longitude: 24.935450 View: Google Map
ails.deviantart.com	ok	IP: 108.156.60.103 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.mansgreback.com	ok	IP: 198.49.23.145 Country: United States of America Region: New York City: New York City Latitude: 40.734699 Longitude: -74.005898 View: Google Map
pousse.rapiere.free.fr	ok	IP: 212.27.63.129 Country: France Region: Ile-de-France City: Paris Latitude: 48.853409 Longitude: 2.348800 View: Google Map
vxresource.wordpress.com	ok	IP: 192.0.78.12 Country: United States of America Region: California City: San Francisco Latitude: 37.748425 Longitude: -122.413673 View: Google Map
opengameart.org	ok	IP: 199.180.155.30 Country: United States of America Region: California City: Los Angeles Latitude: 34.052986 Longitude: -118.263687 View: Google Map

DOMAIN	STATUS	GEOLOCATION
urbalazs.hu	ok	IP: 5.56.37.120 Country: Hungary Region: Pest City: Szigetszentmiklos Latitude: 47.343819 Longitude: 19.043350 View: Google Map
art.gnome.org	ok	IP: 8.43.85.5 Country: United States of America Region: North Carolina City: Raleigh Latitude: 35.773994 Longitude: -78.632759 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
rltiles.sf.net	ok	IP: 204.68.111.100 Country: United States of America Region: California City: San Diego Latitude: 32.799797 Longitude: -117.137047 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	IP: 128.30.52.100 Country: United States of America Region: Massachusetts City: Cambridge Latitude: 42.365078 Longitude: -71.104523 View: Google Map
gulisanolaw.com	ok	IP: 162.241.24.125 Country: United States of America Region: Utah City: Provo Latitude: 40.213909 Longitude: -111.634071 View: Google Map
docs.andorstrail.com	ok	IP: 104.18.1.145 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
code.google.com	ok	IP: 142.250.179.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
forums.rpgmakerweb.com	ok	IP: 45.79.217.141 Country: United States of America Region: Georgia City: Atlanta Latitude: 33.749001 Longitude: -84.387978 View: Google Map
pixeljoint.com	ok	IP: 64.202.191.242 Country: United States of America Region: Arizona City: Scottsdale Latitude: 33.601974 Longitude: -111.887917 View: Google Map
pixelhack.blogspot.com	ok	IP: 142.251.39.97 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

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.