

ANDROID STATIC ANALYSIS REPORT



HoloKenMod (1.6.1)

File Name:	installer344.apk
Package Name:	com.holokenmod
Scan Date:	May 31, 2022, 3:22 p.m.
App Security Score:	40/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	ℚ HOTSPOT
3	4	1	1	1

FILE INFORMATION

File Name: installer344.apk

Size: 0.29MB

MD5: c3d45f2cd6ca5cc7a70e3eb203ec189a

SHA1: e3f6136b55337d62bfad7f8bf9ec3ab80e00f0d9

SHA256: 1ab33b85fe45b595cf9044d72b3e9e8f40f3df21ac49fcda71d88823b0879718

i APP INFORMATION

App Name: HoloKenMod

Package Name: com.holokenmod

Main Activity: com.holokenmod.MainActivity

Target SDK: 22 Min SDK: 8 Max SDK:

Android Version Name: 1.6.1 Android Version Code: 21

APP COMPONENTS

Activities: 4 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: True v3 signature: False

Found 1 unique certificates

Subject: CN=Android Debug, O=Android, C=US

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2020-04-04 20:46:17+00:00 Valid To: 2050-03-28 20:46:17+00:00

Issuer: CN=Android Debug, O=Android, C=US

Serial Number: 0x1 Hash Algorithm: sha1

md5: 3a4f9400c677b0528f9edada48a83aa8

sha1: 16b7b84bffb8a92cbb4c7507d6b146eb4e255d66

sha256: 2c708c236256e6be7687599d6e45580226bb96ee331cdd09d8ac06d75548d2ec

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: fb6b92247335ffa7b8662a939e86d0b0c1802599393926500fb36786ce38f457

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.	
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.	
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.

M APKID ANALYSIS

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

FILE	DETAILS		
	FINDINGS	DETAILS	
classes.dex	Compiler	r8	

△ NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

Q MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.
2	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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	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/holokenmod/GridView.java
2	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/holokenmod/GridView.java com/holokenmod/GridCage.java com/holokenmod/MainActivity.ja va com/holokenmod/SaveGame.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/holokenmod/MainActivity.ja va

■ 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
--------	--------	-------------

DOMAIN	STATUS	GEOLOCATION
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
play.google.com	ok	IP: 142.251.36.46 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.