MOBSF

ANDROID STATIC ANALYSIS REPORT

MasterMindy (20190923)

File Name:	installer3848.apk
Package Name:	eth.matteljay.mastermindy
Scan Date:	May 31, 2022, 6:40 p.m.
App Security Score:	56/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	1	2	1	0

FILE INFORMATION

File Name: installer3848.apk
Size: 1.31MB
MD5: dca2069cc165827e49baf5e7af52d508
SHA1: ed36102765d946483bf8da1c8d78ad0db8cb7889
SHA256: 7912512556f516c12841bd082ef41838d2b8db1931478a0d07be03b1d839e5d3

APP INFORMATION

App Name: MasterMindy
Package Name: eth.matteljay.mastermindy
Main Activity: eth.matteljay.mastermindy.MainActivity
Target SDK: 28
Min SDK: 21
Max SDK:
Android Version Name: 20190923
Android Version Code: 20190923

APP COMPONENTS

Activities: 2
Services: 0
Receivers: 0
Providers: 1
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

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: 2019-12-10 15:36:40+00:00
Valid To: 2047-04-27 15:36:40+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x4dda8c79
Hash Algorithm: sha256
md5: 4878e1c89f8a52107015ee2840049d39
sha1: e562ecc69b874f9764382cfb086ba4880f0a5990
sha256: 6482716a3d6c024ce6740d37e46c2b0cd7725fe8ce5502a91f82a703c8d728be
sha512: bef1575beaee24bd28faec8cff1bcdc6630e3ab7fbab5ea267ab0eabd2d318e9e90c9ecc05f59b793244b341f231254ec5d8d790f467ae68b96f4dd08fa8285c

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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: DETAILS Compiler: r8

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION

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	The App logs information. Sensitive	info	CWE: CWE-532: Insertion of Sensitive Information into Log File	a/a/e/Fa.java a/f/i/g.java a/a/d/a/i.java a/a/d/a/l.java a/n/Z.java a/f/b/a/i.java a/f/c/a/e.java a/a/b/a/a.java a/f/h/h.java a/i/a/t.java a/f/c/e.java a/a/e/S.java a/f/i/c.java a/n/Y.java a/f/c/c.java a/a/a/x.java a/f/c/j.java a/a/a/F.java a/a/e/J.java a/f/h/q.java a/f/g/b.java a/a/e/C0061o.java a/f/c/a/a.java a/n/aa.java b/a/a/a/a/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
	information should never be logged.	info	OWASP MASVS: MSTG-STORAGE-3	a/m/a/C.java a/a/e/C.java a/a/e/ua.java a/o/a/a/k.java a/k/k.java a/a/e/Ia.java a/f/c/f.java a/i/a/ActivityC0081i.java a/a/e/oa.java a/a/d/f.java a/h/b/c.java e/a.java a/a/e/Ba.java a/f/c/b.java a/f/h/b.java a/a/a/C.java a/i/a/C0075c.java a/f/a/e.java a/n/ba.java a/i/a/C0073a.java b/a/a/a/f/a.java a/f/a/c.java a/a/e/U.java a/f/h/e.java a/n/P.java
2	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	c/a/a/o.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
2	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to no hardware resources.
4	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
5	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has no network communications.
6	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files in non-volatile memory.
7	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.
8	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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
schemas.android.com	ok	No Geolocation information available.

EMAILS

EMAIL	FILE
matteljay@pm.me	Android String Resource

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.