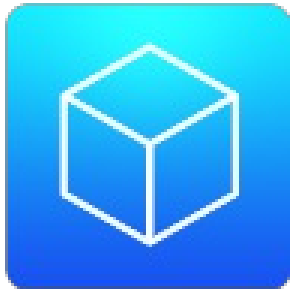
MOBSF

ANDROID STATIC ANALYSIS REPORT



FreeOTP (1.5)

File Name:	FreeOTP.apk
Package Name:	org.fedorahosted.freeotp
Scan Date:	Feb. 28, 2022, 11:55 a.m.
App Security Score:	42/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

HIGH	WARNING	INFO	SECURE
2	1	1	1

FILE INFORMATION

File Name: FreeOTP.apk
Size: 0.43MB
MD5: f79aecc6aca1735e06538c48bb3ce76e
SHA1: eeaed3287bac73b38ea5e396518977c5c8bce937
SHA256: 3324905864a31e1df13771cd657778ac4d80fdf669979b410bfad38eaa9dddb9

APP INFORMATION

App Name: FreeOTP
Package Name: org.fedorahosted.freeotp
Main Activity: org.fedorahosted.freeotp.MainActivity
Target SDK: 20
Min SDK: 14
Max SDK:
Android Version Name: 1.5
Android Version Code: 17

APP COMPONENTS

Activities: 6
Services: 0
Receivers: 0
Providers: 0
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=US, O=Red Hat, Inc., OU=FreeOTP, CN=Red Hat, Inc.
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-11-13 17:46:03+00:00
Valid To: 2041-03-31 17:46:03+00:00
Issuer: C=US, O=Red Hat, Inc., OU=FreeOTP, CN=Red Hat, Inc.
Serial Number: 0x260a0c1d
Hash Algorithm: sha256
md5: 4c552ad349a533bc4d7bb349c4d044c6
sha1: a9902cc2cda835a5b7d3e1f8771f36acb32f29f7
sha256: 01b5d92a368bb99f65123bef732627f6ccc814f27e1490384377445a6f599c49
sha512: 7777c42f88241e133f20f8500dc3863a012fe723ce86a33a5effe2f9914f56cc97c7a242d1e601ece937cb96df1ab96ea3e0cdba77cd2aca26204b20686ab69a

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.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dx (possible dexmerge)</td></tr><tr><td>Manipulator Found</td><td>dexmerge</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
org.fedorahosted.freeotp.MainActivity	Schemes: otpauth://, Hosts: totp, hotp,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

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.
2	Launch Mode of Activity (org.fedorahosted.freeotp.MainActivity) 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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	org/fedorahosted/freeotp/TokenAdapter.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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['camera', 'network connectivity'].
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 user/application initiated 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

DOMAIN	STATUS	GEOLOCATION
lists.fedorahosted.org	ok	**IP:** 38.145.60.21 **Country:** United States of America **Region:** North Carolina **City:** Raleigh **Latitude:** 35.773994 **Longitude:** -78.632759 **View:** Google Map
freeotp.fedorahosted.org	ok	**IP:** 38.145.60.20 **Country:** United States of America **Region:** North Carolina **City:** Raleigh **Latitude:** 35.773994 **Longitude:** -78.632759 **View:** Google Map
fedorahosted.org	ok	**IP:** 67.219.144.68 **Country:** United States of America **Region:** Ohio **City:** Worthington **Latitude:** 40.100941 **Longitude:** -83.014740 **View:** Google Map
www.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"secret" : "Secret"

PLAYSTORE INFORMATION

Title: FreeOTP Authenticator

Score: 3.78 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** 4.0 and up **Category:** Tools **Play Store URL:** org.fedorahosted.freeotp

Developer Details: Red Hat, Red+Hat, None, https://fedorahosted.org/freeotp, freeotp-devel@lists.fedorahosted.org,

Release Date: Nov 13, 2013 **Privacy Policy:** Privacy link

Description:

FreeOTP adds a second layer of security for your online accounts. This works by generating one-time passwords on your mobile devices which can be used in conjunction with your normal password to make your login nearly impossible to hack. These passwords can be generated even when your phone is in airplane mode. FreeOTP works with many of the great online services you already use, including Google, Facebook, Evernote, GitHub and many more! FreeOTP also may work for your private corporate security if they implement the standardized TOTP or HOTP protocols. This includes great enterprise solutions like FreeIPA. FreeOTP is open source and free software! Licensed under the Apache 2.0 license, you can obtain the source code for FreeOTP at https://fedorahosted.org/freeotp for review or modification. Contributions are welcome!
