

#### ANDROID STATIC ANALYSIS REPORT



Yubico Authenticator (2.2.0)

	er350.apk		
Package Name: com.ye	com.yubico.yubioath		
Scan Date: May 3	May 31, 2022, 3:19 p.m.		
App Security Score: 37/	37/100 (HIGH RISK		
Grade:	C		

#### FINDINGS SEVERITY

<b>派</b> HIGH	▲ MEDIUM	<b>i</b> INFO	✓ SECURE	♥ HOTSPOT
4	5	2	1	1

#### FILE INFORMATION

File Name: installer350.apk

Size: 2.54MB

MD5: d4ac0d25aa50f01e38715376847ce48c

**SHA1**: 65a3b443ce9b16d8f90d455c318bd5d9dc6da596

SHA256: 56db44ddd5628395a0d1c0fe36ce61494503ca43ac331e6412c697ed92597476

#### **i** APP INFORMATION

App Name: Yubico Authenticator
Package Name: com.yubico.yubioath

Main Activity: com.yubico.yubioath.ui.main.MainActivity

Target SDK: 29 Min SDK: 15 Max SDK:

Android Version Name: 2.2.0
Android Version Code: 20199

#### **EE** APP COMPONENTS

Activities: 5 Services: 0 Receivers: 0 Providers: 1

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



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: 2013-09-03 14:32:58+00:00 Valid To: 2041-01-19 14:32:58+00:00

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

Serial Number: 0x182c5c3d Hash Algorithm: sha256

md5: cbc761e3082058de3bbc89f59c5a8654

sha1: 0ec2d780ae328df45f7a1072743f46606707eee4

sha256: d8678c5ee2c5e8f80d5d24f664d86ef3f8ed69191489d54d66495f766a256d47

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.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.

## ক্ল APKID ANALYSIS

FILE	DETAILS		
classes.dex	FINDINGS	DETAILS	
Classes.uex	Compiler	unknown (please file detection issue!)	



ACTIVITY	INTENT
com.yubico.yubioath.ui.main.MainActivity	Schemes: https://, Hosts: my.yubico.com,
com.yubico.yubioath.ui.add.AddCredentialActivity	Schemes: otpauth://,

### **△** NETWORK SECURITY

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

## **Q** MANIFEST ANALYSIS

N	O ISSUE		SEVERITY	DESCRIPTION
1	Application Data can be Backed [android:allowBackup=true]	up	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 (com.yubico.yubioath.ui.main.M standard.	ainActivity) is not	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.
3	Launch Mode of Activity (com.yubico.yubioath.ui.add.Add is not standard.	dCredentialActivity)	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.

NO	ISSUE	SEVERITY	DESCRIPTION

4	Activity (com.yubico.yubioath.ui.add.AddCredentialActivity) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.
5	Launch Mode of Activity (com.yubico.yubioath.ui.password.PasswordActivity) 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
				a/f/b/b.java b/a/a/a/b/a.java b/c/a/b/a/c.java a/n/U.java com/yubico/yubioath/ui/main/U.java a/a/d/g.java a/n/ba.java b/c/a/a/a.java a/f/a/a/b.java a/a/a/a/a.java

NO	ISSUE	SEVERITY	STANDARDS	a/n/ca.java <b>析化好多</b> .java a/f/h/b.java
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	a/n/V.java a/f/a/a/h.java b/c/a/b/a/f.java com/yubico/yubioath/ui/add/b.java b/a/a/a/h.java b/c/b/e/t.java a/i/a/ActivityC0046j.java a/f/i/e.java a/f/i/e.java a/f/b/e.java a/f/b/e.java a/f/b/e.java a/h/b/c.java b/c/a/b/b/c.java b/c/a/b/b/c.java b/c/a/b/b/c.java b/i/a/C0037a.java a/i/a/C0037a.java a/i/a/b.java com/yubico/yubioath/ui/main/MainActivity.j ava a/f/b/k.java com/yubico/yubioath/ui/main/T.java com/yubico/yubioath/ui/main/T.java com/yubico/yubioath/ui/main/X.java b/b/a/d.java a/i/a/LayoutInflater\$Factory2C0056u.java a/n/da.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	b/c/b/a/c.java com/yubico/yubioath/ui/password/Passwor dFragment.java
3	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	b/c/b/e/b.java
4	SHA-1 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	b/c/b/a/h.java b/c/b/c/h.java b/c/b/c/f.java b/c/b/c/a.java b/c/b/a/e.java b/c/a/a/a/e.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 invoke platform-provided 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 ['NFC', 'camera', 'USB'].
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_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_CKM.1.1(3),FCS_CKM.1.2(3)	Selection-Based Security Functional Requirements	Password Conditioning	A password/passphrase shall perform [Password-based Key Derivation Functions] in accordance with a specified cryptographic algorithm

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
12	FCS_COP.1.1(4)	Selection-Based Security Functional Requirements	Cryptographic Operation - Keyed-Hash Message Authentication	The application perform keyed-hash message authentication with cryptographic algorithm ['HMAC-SHA1'] .

## **Q DOMAIN MALWARE CHECK**

DOMAIN	STATUS	GEOLOCATION
www.youtube.com	ok	IP: 142.251.36.14  Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
developers.yubico.com	ok	IP: 151.101.194.114 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.yubico.com	ok	IP: 151.101.194.114  Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
schemas.android.com	ok	No Geolocation information available.
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

## **▶** HARDCODED SECRETS

# POSSIBLE SECRETS "credential\_type": "Type" "password": "Password"

#### 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 | <u>Ajin Abraham</u> | <u>OpenSecurity</u>.