MOBSF

ANDROID STATIC ANALYSIS REPORT

Yubico Authenticator (2.2.0)

File Name:	installer3.apk
Package Name:	com.yubico.yubioath
Scan Date:	May 31, 2022, 7:40 a.m.
App Security Score:	33/100 (HIGH RISK)
Grade:	

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
5	5	2	1	1

FILE INFORMATION

File Name: installer3.apk
Size: 2.94MB
MD5: 4617f415214322bb09b19b051efe3f0c
SHA1: 49ff14e319887698534ffa0046e10d3c10992114
SHA256: 710294baa966de2c0e2310453cb0761547ce49179062d1532f59b5b39641e467

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

APP COMPONENTS

Activities: 6
Services: 0
Receivers: 0
Providers: 1
Exported Activities: 1
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: O=Yubico AB, CN=Android code signing
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-03-08 12:48:31+00:00
Valid To: 2037-03-02 12:48:31+00:00
Issuer: O=Yubico AB, CN=Android code signing
Serial Number: 0xf821b31f4c97f2c3
Hash Algorithm: sha1
md5: 7bdc77dbbf556c124f502918454e97a0
sha1: c636f48cb00b49337b6dce958870433f289c827a
sha256: 3e21da5acaa8d49ce515b1c6d2a1903bae298d0911432c55e75a196199f2b9a0
sha512: 090ab0c062aab9b94e1352495a2e1d7bd52cdd4e722bbbd709ed7663608b825c2814253485998d4dcc68c6a906ac678bb87fba11533a2869d1da3235cd64fb86

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.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.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

BROWSABLE ACTIVITIES

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

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 (com.yubico.yubioath.ui.main.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.
3	Launch Mode of Activity (com.yubico.yubioath.ui.add.AddCredentialActivity) 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.
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
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/f/i/t.java b/c/b/a/f.java b/c/a/b/b/c.java a/n/da.java b/a/a/a/f/b/C0214k.java b/a/a/a/h/a/a.java b/c/a/a/a.java b/a/a/a/b/a.java a/l/a/b.java b/b/a/d.java b/a/a/a/f/b/kc.java a/f/g/a.java com/yubico/yubioath/ui/main/U.java a/n/U.java b/a/a/a/f/b/yc.java com/yubico/yubioath/ui/add/b.java b/a/a/a/c/d.java a/i/a/ActivityC0062j.java b/a/a/a/f/f/C0269c.java a/i/a/LayoutInflater$Factory2C0072u.java a/f/i/AbstractC0051b.java b/a/a/a/f/b/C0220m.java a/i/a/C0055c.java a/h/b/c.java a/f/b/f.java a/n/V.java b/c/b/e/q.java b/a/a/a/f/b/uc.java a/a/d/g.java a/f/b/b.java a/f/h/b.java com/yubico/yubioath/ui/main/MainActivity.java b/a/a/b/b/a.java a/n/ba.java a/f/i/e.java a/a/a/a/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a/f/b/e.java a/f/b/g.java b/a/a/a/c/h.java
				a/f/i/v.java com/yubico/yubioath/ui/main/X.java a/n/ca.java b/a/a/a/f/b/C0217l.java b/a/a/a/c/n.java a/i/a/z.java b/a/a/a/c/m.java b/a/a/a/f/b/AbstractC0199f.java b/b/a/e.java b/c/a/b/a/f.java b/c/a/b/a/c.java b/a/a/a/f/f/C0282g.java a/o/a/a/k.java b/a/a/b/a/h.java a/f/a/a/h.java b/a/a/a/f/f/Ac.java b/a/a/a/c/b/a.java b/c/b/e/t.java a/f/b/k.java b/a/a/a/f/b/C0190c.java b/a/a/a/f/f/Da.java com/yubico/yubioath/ui/main/T.java a/i/a/C0053a.java b/a/a/a/c/g.java a/n/ea.java a/f/a/a/b.java
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/PasswordFragment.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/c/h.java b/c/b/a/e.java b/c/b/c/f.java b/c/b/c/a.java b/c/a/a/a/e.java b/c/b/a/h.java
4	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

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.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['NFC', 'camera', 'USB'].

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.
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'] .

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.youtube.com	ok	**IP:** 216.58.214.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developers.yubico.com	ok	**IP:** 151.101.66.114 **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

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	b/a/a/a/c/s.java

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.