ANDROID STATIC ANALYSIS REPORT

 YubiClip (1.2.0)

File Name:	installer342.apk
Package Name:	com.yubico.yubiclip
Scan Date:	May 31, 2022, 4:50 p.m.
App Security Score:	**55/100 (MEDIUM RISK)**
Grade:	B

◕ FINDINGS SEVERITY

🐛 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
1	2	1	1	0

📦 FILE INFORMATION

File Name: installer342.apk
Size: 0.02MB
MD5: 029392e840fa1f5d6bbaa05df9f5b934
SHA1: 2d2debba200c419c483c9144c89ee16c0196ce4a
SHA256: 465bf4079dc834db0639f44a8b889aa53d03dcf4784bb75054b6631fe184b570

ℹ APP INFORMATION

App Name: YubiClip
Package Name: com.yubico.yubiclip
Main Activity: .SettingsActivity
Target SDK: 23
Min SDK: 11
Max SDK:
Android Version Name: 1.2.0
Android Version Code: 5

▦ APP COMPONENTS

Activities: 2
Services: 1
Receivers: 0
Providers: 0
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: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-11-08 22:01:46+00:00
Valid To: 2041-03-26 22:01:46+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x22641686
Hash Algorithm: sha256
md5: a3b543ff7f6ee423999d05237f69c0dc
sha1: 96ad440a51c04bb5a68f2d63909a1b434103a904
sha256: 852408971bed07ebe9e57a3816551e21c7663003bf9f319342ffa456dd3dee69
sha512: 552b928dbc840b9b3c5d241985b929f31c8d6f16e6a718afacd05047159e76d449a327ea69e4a7e68eb90ba6d9ff2bf5bfad310838b334634187b19fa094eb23

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	dx

🗔 BROWSABLE ACTIVITIES

ACTIVITY	INTENT
HandleOTPActivity	Schemes: https://, Hosts: my.yubico.com, Path Prefixes: /neo,

🔒 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	Activity (HandleOTPActivity) 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.

</> 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	com/yubico/yubiclip/ClearClipboardService.java com/yubico/yubiclip/HandleOTPActivity.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 encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

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.