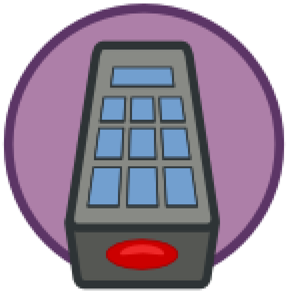
ANDROID STATIC ANALYSIS REPORT



Remote Keyboard (1.6)

File Name:	installer370.apk
Package Name:	de.onyxbits.remotekeyboard
Scan Date:	May 30, 2022, 4:16 p.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	6	1	1	0

FILE INFORMATION

File Name: installer370.apk
Size: 0.4MB
MD5: 318be78be868cea437c23fe8f0248805
SHA1: 100992723f66672ee2f7d8b6d0fea000ca2837bf
SHA256: d19d460b22e352bd4d05a9ae8bcef0d5ede972676d4a07dc246126f0f4766ed2

APP INFORMATION

App Name: Remote Keyboard
Package Name: de.onyxbits.remotekeyboard
Main Activity: de.onyxbits.remotekeyboard.MainActivity
Target SDK: 17
Min SDK: 9
Max SDK:
Android Version Name: 1.6
Android Version Code: 7

APP COMPONENTS

Activities: 5
Services: 1
Receivers: 1
Providers: 0
Exported Activities: 0
Exported Services: 1
Exported Receivers: 1
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: 2013-06-15 16:52:16+00:00
Valid To: 2040-10-31 16:52:16+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x67d315c2
Hash Algorithm: sha256
md5: 3f7dfeb06133dbdb5b7b32106bbcccde
sha1: 2a4aa77beaf2677007cf4a330d152576b1e5c7cc
sha256: 2d7f130cd7b06d012ce3503675e14bd2e2c1822f1a148df8480e5083fb27d1ca
sha512: 9dd460b5ab0300afc93b23b73c9a3142f8c4556ad6cf145993f85f6f2fe61fa1f09fc0639e7c7dfc2f85a9ebedb7c521ea13ed5d767f9143bd1ff69378753a3f

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.BIND_INPUT_METHOD	signature	bind to an input method	Allows the holder to bind to the top-level interface of an input method. Should never be needed for common applications.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<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>
</td></tr>
</table>

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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Service (de.onyxbits.remotekeyboard.RemoteKeyboardService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_INPUT_METHOD [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
3	Broadcast Receiver (de.onyxbits.remotekeyboard.WidgetProvider) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver 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 Broadcast Receiver is explicitly exported.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	de/onyxbits/remotekeyboard/ReplacementActivity.java de/onyxbits/remotekeyboard/TelnetEditorShell.java net/wimpi/telnetd/io/toolkit/Pager.java de/onyxbits/remotekeyboard/Schema.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	net/wimpi/telnetd/io/terminal/Colorizer.java de/onyxbits/remotekeyboard/TelnetEditorShell.java net/wimpi/telnetd/TelnetD.java de/onyxbits/remotekeyboard/RemoteKeyboardService.java de/onyxbits/remotekeyboard/ImportTask.java de/onyxbits/remotekeyboard/Schema.java de/onyxbits/remotekeyboard/CtrlInputAction.java
3	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	de/onyxbits/remotekeyboard/Schema.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 ['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
www.onyxbits.de	ok	**IP:** 212.227.251.101 **Country:** Germany **Region:** Nordrhein-Westfalen **City:** Strang **Latitude:** 51.968700 **Longitude:** 8.753360 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"password" : "Password:"
"password" : "Passwort:"

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.