MOBSF

ANDROID STATIC ANALYSIS REPORT

Fit Notifications (2.9.17)

File Name:	installer194.apk
Package Name:	com.abhijitvalluri.android.fitnotifications
Scan Date:	May 31, 2022, 4:16 p.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	7	1	1	0

FILE INFORMATION

File Name: installer194.apk
Size: 3.93MB
MD5: ec7905409addb4f319d486318790a494
SHA1: bece6617008e494a35dc9f2b2c54287de6006404
SHA256: 09a002bc7e84ac6b22ed63da920d3d605383e55cb0bca60d81716214b5cd6d9f

APP INFORMATION

App Name: Fit Notifications
Package Name: com.abhijitvalluri.android.fitnotifications
Main Activity: com.abhijitvalluri.android.fitnotifications.HomeActivity
Target SDK: 26
Min SDK: 19
Max SDK:
Android Version Name: 2.9.17
Android Version Code: 40

APP COMPONENTS

Activities: 5
Services: 1
Receivers: 1
Providers: 1
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: 2018-09-02 19:42:24+00:00
Valid To: 2046-01-18 19:42:24+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x57846b92
Hash Algorithm: sha256
md5: 43ee970df7fc300b7edeeba9c1ef5f1f
sha1: e9c9a6f35828f6d5197ff2d06bf624efe8aae913
sha256: 071d1112d3a82088b8c9e2b2601f41de9b9edd0c3134a73d3a6283c5369c87d5
sha512: 3c6cf3f59fbb73eeb4cf1df98c609b8963875a64ffad898322b1ae50a06e0796e3f91a248c1fc9e8c71bc184be08a94ece1ed47640fa3881ae97ce008eba38fa

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 (possible dexmerge) Manipulator Found: dexmerge

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	Service (com.abhijitvalluri.android.fitnotifications.services.NLService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NOTIFICATION_LISTENER_SERVICE [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 (com.abhijitvalluri.android.fitnotifications.widget.ServiceToggle) 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
				com/ibm/icu/text/RuleBasedNumberFormat.java com/ibm/icu/impl/ResourceBundleWrapper.java com/abhijitvalluri/android/fitnotifications/services/GenericMessageExtractor.java com/ibm/icu/impl/duration/impl/XMLRecordReader.java com/abhijitvalluri/android/fitnotifications/HomeActivity.java

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	android/databinding/adapters/TextViewBindingAdapter.java com/ibm/icu/impl/Trie2Writable.java com/ibm/icu/impl/ICUDebug.java com/ibm/icu/impl/OlsonTimeZone.java com/abhijitvalluri/android/fitnotifications/utils/TranslitUtil.java com/ibm/icu/impl/text/RbnfScannerProviderImpl.java com/abhijitvalluri/android/fitnotifications/services/IgnoreSummaryMessageExtractor.java com/ibm/icu/impl/ICUService.java com/ibm/icu/text/RBBITableBuilder.java com/ibm/icu/text/RuleBasedBreakIterator.java com/abhijitvalluri/android/fitnotifications/database/AppSelectionDbHelper.java com/ibm/icu/text/RBBISymbolTable.java com/abhijitvalluri/android/fitnotifications/AppChoicesActivity.java com/ibm/icu/impl/StringPrepDataReader.java com/ibm/icu/impl/duration/impl/XMLRecordWriter.java com/ibm/icu/impl/duration/impl/PeriodFormatterData.java com/ibm/icu/text/RBBINode.java com/ibm/icu/impl/URLHandler.java com/ibm/icu/util/VersionInfo.java com/abhijitvalluri/android/fitnotifications/services/BasicMessageExtractor.java com/abhijitvalluri/android/fitnotifications/services/GroupSummaryMessageExtractor.java com/ibm/icu/text/RBBIRuleScanner.java com/abhijitvalluri/android/fitnotifications/services/NLService.java com/abhijitvalluri/android/fitnotifications/utils/AppSelectionsStore.java com/abhijitvalluri/android/fitnotifications/u

NO	ISSUE	SEVERITY	STANDARDS	FILES
				tils/DebugLog.java com/ibm/icu/impl/ICUBinary.java com/ibm/icu/text/CanonicalIterator.java com/ibm/icu/text/PluralSamples.java com/ibm/icu/impl/ICUResourceBundle.java com/ibm/icu/text/RBBISetBuilder.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	com/ibm/icu/impl/CalendarUtil.java com/ibm/icu/text/DateIntervalInfo.java com/ibm/icu/impl/ICUDataVersion.java com/ibm/icu/text/NumberFormat.java com/ibm/icu/util/ULocale.java com/ibm/icu/util/TimeZone.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	com/abhijitvalluri/android/fitnotifications/database/AppSelectionDbHelper.java com/abhijitvalluri/android/fitnotifications/utils/AppSelectionsStore.java
4	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/abhijitvalluri/android/fitnotifications/utils/DebugLog.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 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 implement functionality to encrypt sensitive data 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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
www.fitbit.com	ok	**IP:** 104.16.66.50 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
help.fitbit.com	ok	**IP:** 108.156.60.83 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
lao-dictionary.googlecode.com	ok	**IP:** 142.250.102.82 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 142.251.36.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
casper.beckman.uiuc.edu	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
chasen.aist-nara.ac.jp	ok	**IP:** 163.221.116.25 **Country:** Japan **Region:** Nara **City:** Nara **Latitude:** 34.682999 **Longitude:** 135.800003 **View:** Google Map
opensource.org	ok	**IP:** 104.21.84.214 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
abhijitvalluri.com	ok	**IP:** 198.54.116.205 **Country:** United States of America **Region:** Georgia **City:** Atlanta **Latitude:** 33.727291 **Longitude:** -84.425377 **View:** Google Map
code.google.com	ok	**IP:** 142.250.179.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sourceforge.net	ok	**IP:** 172.64.153.13 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.unicode.org	ok	**IP:** 66.34.208.12 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.814899 **Longitude:** -96.879204 **View:** Google Map
android.abhijitvalluri.com	ok	No Geolocation information available.

EMAILS

EMAIL	FILE
android@abhijitvalluri.com	com/abhijitvalluri/android/fitnotifications/HomeActivity.java
android@abhijitvalluri.com	com/abhijitvalluri/android/fitnotifications/utils/DebugLog.java
c-tsai4@uiuc.edu android@abhijitvalluri.com	Android String Resource

HARDCODED SECRETS

POSSIBLE SECRETS
"disable_forward_screen_on_key" : "disableWhenScreenOn"
"dismiss_relayed_notif_key" : "DismissOtherNotifications"
"display_app_name_key" : "displayAppName"
"done_first_launch_key" : "FirstLaunch"
"forward_priority_only_notifications_key" : "forwardPriorityOnlyNotifications"
"limit_notif_key" : "limitNotifications"
"notif_limit_duration_key" : "NotiflimitDuration"

POSSIBLE SECRETS
"notification_listener_service_state_key" : "NlsState"
"relayed_dismiss_delay_key" : "RelayedDismissDelay"
"show_enabled_apps_key" : "ShowEnabledApps"
"split_notification_key" : "splitNotifications"
"transliterate_notification_key" : "transliterateNotifications"
"version_key" : "AppVersion"

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.