

ANDROID STATIC ANALYSIS REPORT



Missed Notifications Reminder (1.3.2.0.21)

| File Name: | installer252.apk |
|---------------------|-------------------------------------|
| Package Name: | com.app.missednotificationsreminder |
| Scan Date: | May 31, 2022, 11:43 a.m. |
| App Security Score: | 46/100 (MEDIUM RISK) |
| Grade: | |
| | |

FINDINGS SEVERITY

| 派 HIGH | ▲ MEDIUM | i INFO | ✓ SECURE | ♠ HOTSPOT |
|---------------|----------|---------------|----------|-----------|
| 2 | 6 | 1 | 1 | 1 |

FILE INFORMATION

File Name: installer252.apk

Size: 3.83MB

MD5: db4726f36f0000ad724df80d15ffe585

SHA1: 2861192dae67eecc9de17ce74a4583fbb234b7d2

SHA256: cc448fbe6843bf7898092da45a6f8714a37b56f64a8ccbe3d38973b2411b1108

i APP INFORMATION

App Name: Missed Notifications Reminder

Package Name: com.app.missednotificationsreminder

Main Activity: com.app.missednotificationsreminder.ui.activity.SettingsActivity

Target SDK: 27 Min SDK: 18 Max SDK:

Android Version Name: 1.3.2.0.21
Android Version Code: 2010302021

EE APP COMPONENTS

Activities: 3 Services: 6 Receivers: 2 Providers: 2

Exported Activities: O Exported Services: 2 Exported Receivers: O Exported Providers: O

***** 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: 2016-08-10 17:30:03+00:00 Valid To: 2043-12-27 17:30:03+00:00

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

Serial Number: 0x2ea993b5 Hash Algorithm: sha256

md5: 81f9f5665c5c5599df56eca470ccfb20

sha1: 302e94ddc77fe96666e3056917468623ab750ed4

sha256: e37b940e25515999af1cc3ce198c90bac958e0b12f092b24328f2c6188cbab61

| 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.WAKE_LOCK | normal | prevent phone from sleeping | Allows an application to prevent the phone from going to sleep. |
| android.permission.READ_EXTERNAL_STORAGE | dangerous | read external storage contents | Allows an application to read from external storage. |
| android.permission.VIBRATE | normal | control vibrator | Allows the application to control the vibrator. |
| android.permission.ACCESS_NETWORK_STATE | normal | view network status | Allows an application to view the status of all networks. |
| android.permission.RECEIVE_BOOT_COMPLETED | normal | automatically start at boot | Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running. |



| FILE | DETAILS | | | |
|-------------|------------------|----|--|--|
| classes.dex | FINDINGS DETAILS | | | |
| cidsses.uex | Compiler | r8 | | |

△ NETWORK SECURITY

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

Q 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 (com.app.missednotificationsreminder.service.ReminderNotificationListenerService) 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 | Launch Mode of Activity (com.app.missednotificationsreminder.ui.activity.SettingsActivity) 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 | Service (com.evernote.android.job.gcm.PlatformGcmService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_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. |



| 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 | com/wdullaer/materialdatetimepicker/time/Rad ialPickerLayout.java com/app/missednotificationsreminder/ui/activit y/common/AppCompatActivityWithNestedFrag mentFix.java timber/log/Timber.java com/wdullaer/materialdatetimepicker/time/Am PmCirclesView.java com/appyvet/rangebar/RangeBar.java com/tbruyelle/rxpermissions/RxPermissions.jav a com/wdullaer/materialdatetimepicker/time/Rad ialSelectorView.java com/wdullaer/materialdatetimepicker/time/Rad ialTextsView.java com/wdullaer/materialdatetimepicker/time/Circ leView.java com/wdullaer/materialdatetimepicker/date/Day PickerView.java com/wdullaer/materialdatetimepicker/date/Day PickerView.java com/app/missednotificationsreminder/service/ ReminderNotificationListenerService.java com/wdullaer/materialdatetimepicker/time/Tim ePickerDialog.java |
| 2 | 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/evernote/android/job/JobStorage.java |
| 3 | 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 | dagger/internal/Linker.java rx/internal/schedulers/NewThreadWorker.java dagger/internal/ProvidesBinding.java |

| NO | ISSUE | SEVERITY STANDARDS | | FILES |
|----|--|--------------------|---|--|
| 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/jakewharton/u2020/data/LumberYard.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 use no 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 ['network connectivity']. |
| 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. |

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|----|-------------------|--|--|--|
| 7 | 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. |
| 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_HTTPS_EXT.1.2 | Selection-Based Security Functional Requirements | HTTPS Protocol | The application implement HTTPS using TLS. |
| 11 | FCS_HTTPS_EXT.1.3 | Selection-Based Security Functional Requirements | HTTPS Protocol | The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid. |
| 12 | FIA_X509_EXT.2.1 | Selection-Based Security Functional Requirements | X.509 Certificate Authentication | The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS. |

Q DOMAIN MALWARE CHECK

| DOMAIN | STATUS | GEOLOCATION |
|--------|--------|-------------|
| | | |

| DOMAIN | STATUS | GEOLOCATION |
|-------------|--------|--|
| 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 |
| xmlpull.org | ok | IP: 74.50.61.58 Country: United States of America Region: Texas City: Dallas Latitude: 32.814899 Longitude: -96.879204 View: Google Map |

HARDCODED SECRETS

POSSIBLE SECRETS

"mdtp_deleted_key": "%1\$sを削除しました"

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 | Ajin Abraham | OpenSecurity.