# MOBSF

# ANDROID STATIC ANALYSIS REPORT

AN2Linux (0.10.0)

| | |
|---|---|
| File Name: | installer389.apk |
| Package Name: | kiwi.root.an2linuxclient |
| Scan Date: | May 31, 2022, 8:05 a.m. |
| App Security Score: | 59/100 (MEDIUM RISK) |
| Grade: | B |

# FINDINGS SEVERITY

| HIGH | MEDIUM | INFO | SECURE | HOTSPOT |
|---|---|---|---|---|
| 1 | 7 | 1 | 2 | 1 |

# FILE INFORMATION

**File Name:** installer389.apk
**Size:** 2.63MB
**MD5:** 49cc64c4cf1700694ef9715018aa5491
**SHA1:** cf41ef9066652df7964570b5998fd480361fe40e
**SHA256:** 0065045d6d9e6abb461f21929477b29a74f5d953b70b02e11408e205b1493de2

# APP INFORMATION

**App Name:** AN2Linux
**Package Name:** kiwi.root.an2linuxclient
**Main Activity:** kiwi.root.an2linuxclient.activities.MainSettingsActivity
**Target SDK:** 29
**Min SDK:** 18
**Max SDK:**
**Android Version Name:** 0.10.0
**Android Version Code:** 15

# APP COMPONENTS

Activities: 7
Services: 4
Receivers: 1
Providers: 1
Exported Activities: 0
Exported Services: 2
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: 2017-01-04 21:31:27+00:00
Valid To: 2044-05-22 21:31:27+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x1f6f0dcb
Hash Algorithm: sha256
md5: dda008118f190ed9702c49b8cd50220b
sha1: a4536b974e6af2ff015df0cb6ae98a4b4f9694b4
sha256: ccd5fc2826d7f86345d8ee8eb07d25e7b985ce25e38be5578304833a8d05610e
sha512: 35e7687494902d5b833dd9c0e6fef76a57603014371e89c35b2d8fee54f588491b405a173e720b00a7846943816c315cd59712e77e776283018c4bacbbfb4086

| 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.INTERNET | normal | full Internet access | Allows an application to create network sockets. |
| android.permission.BLUETOOTH | normal | create Bluetooth connections | Allows applications to connect to paired bluetooth devices. |
| android.permission.ACCESS_NETWORK_STATE | normal | view network status | Allows an application to view the status of all networks. |
| android.permission.ACCESS_WIFI_STATE | normal | view Wi-Fi status | Allows an application to view the information about the status of Wi-Fi. |
| 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. |
| android.permission.ACCESS_COARSE_LOCATION | dangerous | coarse (network-based) location | Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
| --- | --- | --- | --- |
| android.permission.FOREGROUND_SERVICE | normal | | Allows a regular application to use Service.startForeground. |
| android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS | normal | | Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS. |

# APKID ANALYSIS

| FILE | DETAILS |
| --- | --- |
| classes.dex | FINDINGS: Compiler — DETAILS: r8 |

# 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 | Broadcast Receiver (kiwi.root.an2linuxclient.utils.BootReceiver) 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. |
| 3 | Service (kiwi.root.an2linuxclient.utils.NotificationService) 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. |
| 4 | Service (kiwi.root.an2linuxclient.utils.AN2LinuxTileService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_QUICK_SETTINGS_TILE [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. |

## </> 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<br>OWASP MASVS: MSTG-STORAGE-3 | b/h/e/i.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')<br>OWASP Top 10: M7: Client Code Quality | d/a/a/d/i.java |
| 3 | The App uses an insecure Random Number Generator. | warning | CWE: CWE-330: Use of Insufficiently Random Values<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-6 | d/a/a/c/a.java |
| 4 | This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel. | secure | OWASP MASVS: MSTG-NETWORK-4 | d/a/a/c/a.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. |

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---|---|---|---|---|
| 3 | FCS_CKM_EXT.1.1 | Security Functional Requirements | Cryptographic Key Generation Services | The application implement asymmetric key generation. |
| 4 | FDP_DEC_EXT.1.1 | Security Functional Requirements | Access to Platform Resources | The application has access to ['network connectivity', 'bluetooth', 'location']. |
| 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 user/application initiated network communications. |
| 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 not encrypt any data in traffic or does not transmit any data 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. |

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---|---|---|---|---|
| 11 | FCS_CKM.1.1(1) | Selection-Based Security Functional Requirements | Cryptographic Asymmetric Key Generation | The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower. |
| 12 | 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.. |
| 13 | FCS_COP.1.1(2) | Selection-Based Security Functional Requirements | Cryptographic Operation - Hashing | The application perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1/SHA-256/SHA-384/SHA-512 and message digest sizes 160/256/384/512 bits. |
| 14 | 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. |
| 15 | FIA_X509_EXT.1.1 | Selection-Based Security Functional Requirements | X.509 Certificate Validation | The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The application validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates', 'The certificate path must terminate with a trusted CA certificate']. |
| 16 | FIA_X509_EXT.1.2 | Selection-Based Security Functional Requirements | X.509 Certificate Validation | The application treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE. |
| 17 | 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. |

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---|---|---|---|---|
| 18 | FIA_X509_EXT.2.2 | Selection-Based Security Functional Requirements | X.509 Certificate Authentication | When the application cannot establish a connection to determine the validity of a certificate, the application allow the administrator to choose whether to accept the certificate in these cases or accept the certificate ,or not accept the certificate. |
| 19 | FCS_CKM.1.1(2) | Optional Security Functional Requirements | Cryptographic Symmetric Key Generation | The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit. |

# DOMAIN MALWARE CHECK

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| github.com | ok | **IP:** 140.82.121.4<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| www.gnu.org | ok | **IP:** 209.51.188.116<br>**Country:** United States of America<br>**Region:** Massachusetts<br>**City:** Boston<br>**Latitude:** 42.358429<br>**Longitude:** -71.059769<br>**View:** Google Map |
| schemas.android.com | ok | No Geolocation information available. |

# HARDCODED SECRETS

| POSSIBLE SECRETS |
| --- |
| "certificate" : "certificate" |
| "device_key_and_cert" : "device_key_and_cert" |
| "main_changelog_key" : "main_changelog_key" |
| "main_display_test_notification_key" : "main_display_test_notification_key" |
| "main_license_key" : "main_license_key" |
| "main_setup_category_key" : "main_setup_category_key" |
| "open_ignore_battery_optimization_settings_key" : "open_ignore_battery_optimization_settings_key" |
| "privatekey" : "privatekey" |

---

## 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.