# ANDROID STATIC ANALYSIS REPORT

## Chiaki (1.3.0)

| | |
|---|---|
| File Name: | installer73.apk |
| Package Name: | com.metallic.chiaki |
| Scan Date: | May 31, 2022, 9:22 a.m. |
| App Security Score: | 64/100 (LOW RISK) |
| Grade: | A |

# FINDINGS SEVERITY

| HIGH | MEDIUM | INFO | SECURE | HOTSPOT |
|---|---|---|---|---|
| 0 | 4 | 1 | 1 | 0 |

# FILE INFORMATION

**File Name:** installer73.apk
**Size:** 8.02MB
**MD5:** 4a30ac42a0a27aa0d93e843d3b6cf724
**SHA1:** 9fa40e46bbc7f9f24b7964dc7cd6f641c671d580
**SHA256:** 12dd9e2dfe61050c5e02d7311498852263b18ece34dcff8cbc5f4592bbf25c6f

# APP INFORMATION

**App Name:** Chiaki
**Package Name:** com.metallic.chiaki
**Main Activity:** com.metallic.chiaki.main.MainActivity
**Target SDK:** 29
**Min SDK:** 21
**Max SDK:**
**Android Version Name:** 1.3.0
**Android Version Code:** 7

# APP COMPONENTS

**Activities:** 6
**Services:** 1
**Receivers:** 0
**Providers:** 2
**Exported Activities:** 0
**Exported Services:** 0
**Exported Receivers:** 0
**Exported Providers:** 0

# CERTIFICATE INFORMATION

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=DE, CN=Florian Märkl
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-11-01 16:51:41+00:00
Valid To: 2044-10-25 16:51:41+00:00
Issuer: C=DE, CN=Florian Märkl
Serial Number: 0xe6c2cb1
Hash Algorithm: sha256
md5: 97db35e4218ef20f474e0436a05f4f0b
sha1: 6a3623112522b287fca2e11d1eeeedc2e45dbd54
sha256: 3108372edcfe425169cc72f4481e76a724f5d5e4c953250411e134a9e48dcbbb
sha512: f5fd455f4df50b1782d05aeb82d9d62f15cc805711a1c0949715299a53b3ad0ef9c1638066b231aa52a3e1715d3a3b905f08ae80865bbb68e8021890b0eccdf2
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 52ab2f3bce61b5370ee8b70fbcd03cc7f4e37f39bd80371bf17e0c5505f64433
```

| TITLE | SEVERITY | DESCRIPTION |
|---|---|---|
| Signed Application | info | Application is signed with a code signing certificate |
| Application vulnerable to Janus Vulnerability | warning | 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.ACCESS_NETWORK_STATE | normal | view network status | Allows an application to view the status of all networks. |

## APKID ANALYSIS

<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>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8</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. |

## CODE ANALYSIS

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 1 | IP Address disclosure | warning | CWE: CWE-200: Information Exposure<br>OWASP MASVS: MSTG-CODE-2 | com/metallic/chiaki/regist/RegistActivity.java<br>com/metallic/chiaki/discovery/DiscoveryManager.java |
| 2 | 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 | com/metallic/chiaki/manualconsole/EditManualConsoleViewModel$existingHost$1.java<br>com/metallic/chiaki/regist/RegistExecuteViewModel.java<br>com/metallic/chiaki/discovery/DiscoveryManager.java<br>com/metallic/chiaki/lib/DiscoveryService.java<br>com/metallic/chiaki/common/SerializedSettingsKt.java |

# SHARED LIBRARY BINARY ANALYSIS

| NO | SHARED OBJECT | NX | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|
| 1 | lib/armeabi-v7a/libchiaki-jni.so | True<br>info<br>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | True<br>info<br>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The shared object does not have run-time search path or RPATH set. | None<br>info<br>The shared object does not have RUNPATH set. | True<br>info<br>The shared object has the following fortified functions: ['__strlen_chk', '__memset_chk', '__vsnprintf_chk', '__memcpy_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__vsprintf_chk'] | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|
| 2 | lib/x86/libchiaki-jni.so | True<br>info<br>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | True<br>info<br>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The shared object does not have run-time search path or RPATH set. | None<br>info<br>The shared object does not have RUNPATH set. | True<br>info<br>The shared object has the following fortified functions: ['__strlen_chk', '__memset_chk', '__vsnprintf_chk', '__memcpy_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__vsprintf_chk'] | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|
| 3 | lib/arm64-v8a/libchiaki-jni.so | True<br>info<br>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | True<br>info<br>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The shared object does not have run-time search path or RPATH set. | None<br>info<br>The shared object does not have RUNPATH set. | True<br>info<br>The shared object has the following fortified functions: ['__FD_ISSET_chk', '__vsprintf_chk', '__memmove_chk', '__memset_chk', '__memcpy_chk', '__FD_SET_chk', '__vsnprintf_chk', '__read_chk', '__strlen_chk'] | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|
| 4 | lib/x86_64/libchiaki-jni.so | True<br>info<br>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | True<br>info<br>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return. | Full RELRO<br>info<br>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None<br>info<br>The shared object does not have run-time search path or RPATH set. | None<br>info<br>The shared object does not have RUNPATH set. | True<br>info<br>The shared object has the following fortified functions: ['__strlen_chk', '__memset_chk', '__vsnprintf_chk', '__memcpy_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__vsprintf_chk', '__read_chk', '__memmove_chk'] | True<br>info<br>Symbols are stripped. |

## 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. |

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---|---|---|---|---|
| 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 user/application initiated network communications. |
| 7 | FDP_DAR_EXT.1.1 | Security Functional Requirements | Encryption Of Sensitive Application Data | The application does not encrypt files 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. |

# 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 |

## HARDCODED SECRETS

| POSSIBLE SECRETS |
|---|
| "preferences_bitrate_key" : "stream_bitrate" |
| "preferences_discovery_enabled_key" : "discovery_enabled" |
| "preferences_export_settings_key" : "export_settings" |
| "preferences_fps_key" : "stream_fps" |
| "preferences_import_settings_key" : "import_settings" |
| "preferences_log_verbose_key" : "log_verbose" |
| "preferences_on_screen_controls_enabled_key" : "on_screen_controls_enabled" |
| "preferences_resolution_key" : "stream_resolution" |

| POSSIBLE SECRETS |
|---|
| "preferences_swap_cross_moon_key" : "swap_cross_moon" |
| "preferences_touchpad_only_key" : "touchpad_only_enabled" |

## 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.