# ANDROID STATIC ANALYSIS REPORT

## MasterMindy (20190923)

| | |
|---|---|
| File Name: | installer3849.apk |
| Package Name: | eth.matteljay.mastermindy |
| Scan Date: | May 31, 2022, 6:38 p.m. |
| App Security Score: | 73/100 (LOW RISK) |
| Grade: | A |

# FINDINGS SEVERITY

| HIGH | MEDIUM | INFO | SECURE | HOTSPOT |
|---|---|---|---|---|
| 0 | 2 | 2 | 1 | 0 |

# FILE INFORMATION

**File Name:** installer3849.apk
**Size:** 1.31MB
**MD5:** eceb3e68a2ae554ee1eca29222253641
**SHA1:** 51d0e78c24fade9af9048d6c20ea7b64e9162ee2
**SHA256:** 3b66c6a4a70c2e728db69fc4eb7e0aad839339a7b45c1f30887ba2ba6e7cbac7

# APP INFORMATION

**App Name:** MasterMindy
**Package Name:** eth.matteljay.mastermindy
**Main Activity:** eth.matteljay.mastermindy.MainActivity
**Target SDK:** 28
**Min SDK:** 21
**Max SDK:**
**Android Version Name:** 20190923
**Android Version Code:** 20190923

## APP COMPONENTS

**Activities:** 2
**Services:** 0
**Receivers:** 0
**Providers:** 1
**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=NL, ST=Provinciale, L=LocaCity, O=Organii, OU=TheUnit, CN=Mat Teljay
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-09-04 22:02:56+00:00
Valid To: 2163-07-31 22:02:56+00:00
Issuer: C=NL, ST=Provinciale, L=LocaCity, O=Organii, OU=TheUnit, CN=Mat Teljay
Serial Number: 0x257933a
Hash Algorithm: sha256
md5: d2904d04a6befe20581ae3ce107928a6
sha1: 7d3ad3e34cbc217e15c8252aa5a22d303c7367d9
sha256: 3acd00504f57b6a8059dbfba60fc82dbed92316abbcf53929d5199ae6814364c
sha512: 52bbfd9e12b0f52dc3aacc8a0d95951a717b3b6f5dd3d891442029e4377cf49cdc6b0a2c4a052b90285076c06f703baa2770c42d175113b8668a6978e5df4228
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: aa6298c275d7519d5e40c3c202661180aeac3c8a07adbda280dcd605b96bd7f7
```

| 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. |

## 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>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 | The App logs information. Sensitive | info | CWE: CWE-532: Insertion of Sensitive Information into Log File | a/f/h/h.java<br>a/f/c/c.java<br>a/a/a/F.java<br>a/i/a/C0075c.java<br>a/m/a/C.java<br>a/i/a/C0073a.java<br>a/n/ba.java<br>a/f/c/j.java<br>a/f/g/b.java<br>a/n/P.java<br>a/a/e/J.java<br>a/a/e/C0061o.java<br>a/f/h/q.java<br>a/a/d/a/i.java<br>a/f/c/a/e.java<br>a/a/d/a/l.java<br>a/a/e/C.java<br>a/a/e/ua.java<br>a/n/Z.java<br>b/a/a/a/f/a.java<br>a/h/b/c.java<br>a/i/a/t.java<br>a/a/e/la.java<br>a/f/c/f.java<br>a/a/e/oa.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 1 | information should never be logged. | info | OWASP MASVS: MSTG-STORAGE-3 | a/n/Y.java<br>a/f/b/a/i.java<br>a/a/d/f.java<br>a/a/a/C.java<br>a/a/e/Ba.java<br>a/a/b/a/a.java<br>a/f/a/e.java<br>a/f/c/b.java<br>a/f/a/c.java<br>a/f/h/b.java<br>a/a/e/U.java<br>a/a/a/x.java<br>a/n/aa.java<br>a/a/e/Fa.java<br>a/f/i/c.java<br>a/f/h/e.java<br>e/a.java<br>a/k/k.java<br>a/f/i/g.java<br>a/i/a/ActivityC0081i.java<br>a/o/a/a/k.java<br>a/f/c/a/a.java<br>b/a/a/a/a/h.java<br>a/f/c/e.java<br>a/a/e/S.java |
| 2 | This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it. | info | OWASP MASVS: MSTG-STORAGE-10 | c/a/a/o.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. |
| 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 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 |
|---|---|---|
| schemas.android.com | ok | No Geolocation information available. |

## EMAILS

| EMAIL | FILE |
|---|---|
| matteljay@pm.me | Android String Resource |

### 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.