MOBSF

ANDROID STATIC ANALYSIS REPORT

Stratum 0 Widget (6.1.0-foss)

File Name:	installer373.apk
Package Name:	horse.amazin.my.stratum0.statuswidget
Scan Date:	May 30, 2022, 3:37 p.m.
App Security Score:	57/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	9	3	2	0

FILE INFORMATION

File Name: installer373.apk
Size: 1.74MB
MD5: 3439798e814af3b0c7f6cad0f99dda0f
SHA1: 6e4c7481e16c693dcb66f012d11dfd821813c43a
SHA256: e33361c29d4736f8319f61eeecc5102bee0baa4c3b09d278d24c046eb857d61b

APP INFORMATION

App Name: Stratum 0 Widget
Package Name: horse.amazin.my.stratum0.statuswidget
Main Activity: horse.amazin.my.stratum0.statuswidget.ui.StatusActivity
Target SDK: 29
Min SDK: 21
Max SDK:
Android Version Name: 6.1.0-foss
Android Version Code: 24

APP COMPONENTS

Activities: 2
Services: 7
Receivers: 3
Providers: 1
Exported Activities: 0
Exported Services: 0
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=Vincent Breitmoser
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-12-05 20:21:47+00:00
Valid To: 2042-11-29 20:21:47+00:00
Issuer: CN=Vincent Breitmoser
Serial Number: 0x5fd6c86f
Hash Algorithm: sha256
md5: 2175053efa143728fefeb889b113ac3a
sha1: 96fd312ea8754a4ec93648174525e9a77c39145c
sha256: c6c24cec88032e47600b26b1e0c7a077b75af484c07e3997b30f5fe9a46b1569
sha512: 4b31a60b4f94757a327ca4707a59687333eefb138117794e0e234e4d5ab969a3f85b2895aefecd20827c3f7ea25c6c8e939703228910abfbc8824d0e3d2acf37
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 61c50e761e34975c61def2d48a5161ed6b0e391e3574fddd687d9179998c41bc

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.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MANUFACTURER check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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	Broadcast Receiver (horse.amazin.my.stratum0.statuswidget.service.Stratum0WidgetProvider) 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	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	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. 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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	j/a/a/f3/f.java j/a/a/b3/q.java j/a/a/h3/f/d.java j/a/a/k2/a.java j/a/a/a3/b.java j/a/a/n2/a.java j/a/j/a/e.java j/a/a/r2/a.java j/a/a/i3/w0.java j/a/a/c3/a.java j/a/a/s2/a.java j/a/a/h3/f/b.java j/a/a/o2/a.java j/a/a/i3/y0.java j/a/a/i2/b.java j/a/a/j3/o.java j/a/a/e3/b.java j/a/a/i3/s.java j/a/a/t2/a.java j/a/a/d3/d.java j/a/a/v2/a.java j/a/a/w2/c.java j/a/a/i3/v0.java j/a/a/z2/a.java j/a/a/i3/u0.java j/a/a/x2/b.java j/a/a/l2/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	j/a/j/d/a/j.java a/c/f/b.java b/a/a/b/f/a.java a/f/a/b.java b/a/a/b/b/p.java b/a/b/c.java a/c/e/b.java b/a/a/b/b/h.java j/c/d/g.java b/a/a/b/d/c/l.java a/c/c/a.java b/a/a/b/e/b/a.java a/d/a/m.java b/a/a/a/i/t/a.java b/a/a/b/b/o.java a/d/a/a.java a/d/a/j.java a/d/a/e.java b/a/a/b/b/g.java b/a/a/b/b/d.java a/d/a/b.java
3	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	h/e0/i/i/b.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	h/e0/i/c.java h/e0/i/h.java h/e0/i/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	b/a/a/a/i/v/j/z.java b/a/a/a/i/v/j/e0.java b/a/a/a/i/v/j/d0.java
6	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	j/a/f/d/b.java j/a/f/b/e.java j/a/f/b/f.java j/a/a/f3/e.java
7	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	horse/amazin/my/stratum0/status widget/ui/StatusActivity.java horse/amazin/my/stratum0/status widget/d/d.java
8	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	horse/amazin/my/stratum0/status widget/ui/StatusActivity.java
9	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	g/b/c/l/e/i.java
10	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	g/b/c/h/p.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 implement 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 implement asymmetric key generation.
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 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.
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(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode or AES-GCM (as defined in NIST SP 800-38D) and cryptographic key sizes 256-bit/128-bit.
14	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
15	FCS_COP.1.1(4)	Selection-Based Security Functional Requirements	Cryptographic Operation - Keyed-Hash Message Authentication	The application perform keyed-hash message authentication with cryptographic algorithm ['HMAC-SHA1'] .
16	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
17	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.
18	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'].
19	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.
20	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.
21	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.
22	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
www.slf4j.org	ok	**IP:** 83.166.144.67 **Country:** Switzerland **Region:** Geneve **City:** Carouge **Latitude:** 46.180962 **Longitude:** 6.139210 **View:** Google Map
status.stratum0.org	ok	**IP:** 144.76.9.122 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map

EMAILS

EMAIL	FILE
ssh-rsa-cert-v01@openssh.com ssh-dss-cert-v01@openssh.com	g/b/c/h/i.java
curve25519-sha256@libssh.org	g/b/c/k/o/e.java
keepalive@openssh.com	g/b/b/d.java
u0013android@android.com0 u0013android@android.com	b/a/a/b/b/u.java

EMAIL	FILE
llman-group14-sha256@ssh.com llman-group15-sha256@ssh.com llman-group15-sha384@ssh.com llman-group16-sha384@ssh.com llman-group16-sha512@ssh.com llman-group18-sha512@ssh.com	b/b/a/c/c/c.java
hmac-md5-96-etm@openssh.com hmac-md5-etm@openssh.com hmac-ripemd160-etm@openssh.com hmac-ripemd160@openssh.com hmac-sha1-96@openssh.com hmac-sha1-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com	b/b/a/c/d/a.java

HARDCODED SECRETS

POSSIBLE SECRETS
"toast_pwd_ok" : "Authorized!"

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.