MobSF

ANDROID STATIC ANALYSIS REPORT

Stratum 0 Widget (5.0.0-foss)

File Name:	installer30.apk
Package Name:	horse.amazin.my.stratum0.statuswidget
Scan Date:	May 31, 2022, 3:09 p.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
2	5	3	2	0

FILE INFORMATION

File Name: installer30.apk
Size: 0.27MB
MD5: 9a3afc50e2d7a1be05b018654fd288ad
SHA1: 96c4c2e9da22e7967692e74cdee1a5edf92fa7bd
SHA256: 710c98f5e1c9599239e8b16b1d546d5205517ff631207333dc23ea410ec13d94

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: 27
Min SDK: 21
Max SDK:
Android Version Name: 5.0.0-foss
Android Version Code: 22

APP COMPONENTS

Activities: 1
Services: 3
Receivers: 1
Providers: 0
Exported Activities: 0
Exported Services: 0
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: 2018-06-20 14:37:35+00:00
Valid To: 2045-11-05 14:37:35+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x3af67a93
Hash Algorithm: sha256
md5: 0672843e61fe141f687f74b681064265
sha1: d52abb1133e25bb9fbd6798eba514406dd99fe20
sha256: d6878b50bd15a3bc178af94d73f8fad51b19233643aeac375f293ee2424bc555
sha512: ace7c47b34f0f390943d5745898458b11d73afdc8451fe3da8f359c4d1456dcef5015dbbeaebf6b467a3c09021758fd694046410bf59df43fd91a1e756c4d054

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.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>Compiler</td><td>dx</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] 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.
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.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

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	horse/amazin/my/stratum0/statuswidget/a/b.java com/jcraft/jsch/jcraft/HMACSHA1.java com/jcraft/jsch/DHECN.java com/jcraft/jsch/jce/SHA512.java com/jcraft/jsch/DHG14.java com/jcraft/jsch/DHG1.java com/jcraft/jsch/KeyExchange.java com/jcraft/jsch/jce/MD5.java com/jcraft/jsch/DHGEX.java com/jcraft/jsch/KeyPair.java com/jcraft/jsch/jce/SHA1.java com/jcraft/jsch/jce/SHA256.java com/jcraft/jsch/jcraft/HMACMD5.java com/jcraft/jsch/jce/HMAC.java com/jcraft/jsch/Session.java com/jcraft/jsch/KnownHosts.java com/jcraft/jsch/jcraft/Compression.java com/jcraft/jsch/jce/SHA384.java
2	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	com/jcraft/jsch/jcraft/HMACSHA1.java com/jcraft/jsch/jce/PBKDF.java com/jcraft/jsch/jce/SHA1.java com/jcraft/jsch/jce/SignatureRSA.java com/jcraft/jsch/jce/SignatureDSA.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/jcraft/jsch/ChannelX11.java com/jcraft/jsch/ChannelForwardedTCPIP.java com/jcraft/jsch/ChannelDirectTCPIP.java com/jcraft/jsch/PortWatcher.java com/jcraft/jsch/jgss/GSSContextKrb5.java com/jcraft/jsch/Session.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	Weak Encryption algorithm used	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/jcraft/jsch/jce/TripleDESCBC.java com/jcraft/jsch/jce/TripleDESCTR.java com/jcraft/jsch/jce/ARCFOUR256.java com/jcraft/jsch/jce/ARCFOUR128.java com/jcraft/jsch/jce/ARCFOUR.java
5	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/statuswidget/a/c.java horse/amazin/my/stratum0/statuswidget/ui/StatusActivity.java
6	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	com/jcraft/jsch/jce/MD5.java com/jcraft/jsch/jcraft/HMACMD5.java
7	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	b/v.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/statuswidget/ui/StatusActivity.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

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.
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(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..
12	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption not in accordance with FCS_COP.1.1(1), AES-ECB mode is being used.
13	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.
14	FCS_COP.1.1(3)	Selection-Based Security Functional Requirements	Cryptographic Operation - Signing	The application perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
15	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
16	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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
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
posix-rename@openssh.com statvfs@openssh.com hardlink@openssh.com	com/jcraft/jsch/ChannelSftp.java
auth-agent-req@openssh.com	com/jcraft/jsch/RequestAgentForwarding.java

EMAIL	FILE
auth-agent@openssh.com	com/jcraft/jsch/ChannelAgentForwarding.java
auth-agent@openssh.com	com/jcraft/jsch/Channel.java
zlib@openssh.com	com/jcraft/jsch/OpenSSHConfig.java
keepalive@jcraft.com no-more-sessions@openssh.com zlib@openssh.com auth-agent@openssh.com	com/jcraft/jsch/Session.java
zlib@openssh.com	com/jcraft/jsch/JSch.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.