

ANDROID STATIC ANALYSIS REPORT



UniPatcher (0.16)

File Name:	installer245.apk		
Package Name:	org.emunix.unipatcher		
Scan Date:	May 31, 2022, 10:54 a.m.		
App Security Score:	52/100 (MEDIUM RISK)		
Grade:			

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	♥ HOTSPOT
1	6	2	1	1

FILE INFORMATION

File Name: installer245.apk

Size: 1.81MB

MD5: ba4d857a6c835dc357c585eb56aa25ff

SHA1: b1af5d69ce76e99e3a9528af7f5110376e8dbdfd

SHA256: 143daeab1773dc8707d3c2c6612f8cb4fa97c346bb51f528cdbabc85eac28bb4

i APP INFORMATION

App Name: UniPatcher

Package Name: org.emunix.unipatcher

Main Activity: org.emunix.unipatcher.ui.activity.MainActivity

Target SDK: 27 Min SDK: 21 Max SDK:

Android Version Name: 0.16
Android Version Code: 160000

APP COMPONENTS

Activities: 5 Services: 1 Receivers: 0 Providers: 0

Exported Activities: O Exported Services: O Exported Receivers: O Exported Providers: O



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: 2017-04-17 19:42:16+00:00 Valid To: 2044-09-02 19:42:16+00:00

Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Serial Number: 0x3df63e90 Hash Algorithm: sha256

md5: 6d93613fd549a19bc113ff0f353d740e

sha1: e5b9703f639bb4bb1fae4d162ba128b75de17586

sha256: febcbed69a1f017f79a17a1c1fe30a46ba4f9f9e0a91d6b5be2e2c2cd8695bf6

sha512: e61e0b4af045ba65cfd810e7030384a10d8ea8debc344d611e9b2b490a35f7eb7e6ff8788fd32453aeb332ef5ed5ac37889bce2c86da69f70b63e14ef4f3f882

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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

M APKID ANALYSIS

FILE	DETAILS		
classes.dex	FINDINGS DETAILS		
Clusses.ucx	Compiler	dx	

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
org.emunix.unipatcher.ui.activity.MainActivity	Schemes: file://, Hosts: *, Mime Types: */*, Path Patterns: /.*\\.aps, /.*\\.ips, /.*\\.ups, /.*\\.bps, /.*\\.ppf, /.*\\.ebp, /.*\\.dps, /.*\\.xdelta, /.*\\.xdelta3, /.*\\.xd, /.*\\.vcdiff,

△ NETWORK SECURITY

NO SCOPE	SEVERITY	DESCRIPTION
----------	----------	-------------

Q MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION

</> 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	org/emunix/unipatcher/b.java me/zhanghai/android/materialprogressbar/Materi alProgressBar.java org/b/d.java org/sufficientlysecure/a/a/a/d.java org/emunix/unipatcher/ui/b/h.java com/afollestad/materialdialogs/internal/g.java me/zhanghai/android/materialprogressbar/BasePr ogressLayerDrawable.java org/emunix/unipatcher/ui/b/l.java org/sufficientlysecure/a/i.java org/sufficientlysecure/a/d.java org/sufficientlysecure/a/j.java org/sufficientlysecure/a/j.java org/emunix/unipatcher/ui/b/c.java org/emunix/unipatcher/ui/b/g.java org/emunix/unipatcher/ui/b/m.java org/emunix/unipatcher/ui/b/m.java org/emunix/unipatcher/ui/b/m.java org/emunix/unipatcher/ui/b/a.java org/emunix/unipatcher/ui/b/a.java org/emunix/unipatcher/ui/b/d.java
2	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	org/emunix/unipatcher/a/c.java org/emunix/unipatcher/patcher/h.java
3	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	org/emunix/unipatcher/patcher/h.java org/emunix/unipatcher/ui/activity/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	org/emunix/unipatcher/ui/activity/b.java org/sufficientlysecure/a/a/a/o.java
5	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	org/sufficientlysecure/a/g.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	org/emunix/unipatcher/ui/activity/MainActivity.jav a
7	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	org/emunix/unipatcher/ui/activity/FilePickerActivit y.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED	
----	---------------	----	-----------------	-------	-------	---------	---------	---------------------	--

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/armeabi-v7a/libxdelta3.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info 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 info 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 info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/x86/libxdelta3.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info 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 info 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 info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

■ NIAP ANALYSIS v1.3

NO	FEATURE DESCRIPTION	
----	---------------------	--

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.
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 no hardware resources.
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 no 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	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.
11	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.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.websequencediagrams.com	ok	IP: 172.105.27.183 Country: Canada Region: Ontario City: Toronto Latitude: 43.700111 Longitude: -79.416298 View: Google Map
www.paypal.com	ok	IP: 151.101.1.21 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
yuml.me	ok	IP: 198.27.83.55 Country: Canada Region: Quebec City: Beauharnois Latitude: 45.316780 Longitude: -73.865898 View: Google Map
maps.google.com	ok	IP: 216.58.208.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
github.com	ok	IP: 140.82.121.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

EMAILS

EMAIL	FILE
btimofeev@emunix.org	org/emunix/unipatcher/ui/activity/DonateActivity.java

EMAIL	FILE
unipatcher@gmail.com	Android String Resource

▶ HARDCODED SECRETS

POSSIBLE SECRETS
"donationsbitcoin" : "Bitcoin"
"donationsbitcoin" : "Bitcoin"
"donationsbitcoin" : "Bitcoin"
"donations_bitcoin" : "Биткоин"

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.

© 2022 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.