MOBSF

ANDROID STATIC ANALYSIS REPORT

UniPatcher (0.17.1)

File Name:	installer212.apk
Package Name:	org.emunix.unipatcher
Scan Date:	May 30, 2022, 3:54 p.m.
App Security Score:	60/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	6	2	1	1

FILE INFORMATION

File Name: installer212.apk
Size: 2.69MB
MD5: 946098456ef71235f75413dea8908f91
SHA1: e8885dbb910cdd2c06f175fcec06f4d61a13c6ae
SHA256: 2d15b867527b0575707a6affbb43c6e2568c1c6e5aa49446bf21b487b0f119b6

APP INFORMATION

App Name: UniPatcher
Package Name: org.emunix.unipatcher
Main Activity: org.emunix.unipatcher.ui.activity.MainActivity
Target SDK: 30
Min SDK: 21
Max SDK:
Android Version Name: 0.17.1
Android Version Code: 170100

APP COMPONENTS

Activities: 5
Services: 2
Receivers: 1
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=ru, CN=Boris Timofeev
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-12-24 16:55:49+00:00
Valid To: 2037-12-18 16:55:49+00:00
Issuer: C=ru, CN=Boris Timofeev
Serial Number: 0x74af7e16
Hash Algorithm: sha256
md5: 6aff899f1b4e8dc5bbb550c3e57a5515
sha1: c31cb23d974f426b38d7af0848a6f1066fcf1fd9
sha256: d7fd9058ef94176c4bf2219a10618eae572cb79b3269b5a6dec2c376d0481e1b
sha512: ed7cb5cdc7fee6f70693c7f52b41705669269b622ab0a443bb217105f5a80171aa8041c8024e2a94916e825dbf215d46fb0b6eabfb91a74fa3729cc2a05bb6e1
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 9676d0c2c22f6c73c900399794fa3bbd8a94cf22efd57d13c31c4a1a2d91cea6

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
com.android.vending.BILLING	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check FINDINGS: Anti Debug Code — DETAILS: Debug.isDebuggerConnected() check FINDINGS: Compiler — DETAILS: r8

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	f/v/f/a.java f/v/a.java f/v/c.java f/v/b.java org/emunix/unipatcher/ui/activity/MainActivity.java
				c/a/a/a/a/a/b.java b/h/j/c/a.java b/h/r/e.java b/h/r/i0.java c/a/a/b/c0/j.java b/h/r/l0.java c/a/a/b/a0/d.java b/h/k/p.java b/b/k/a/b.java b/p/o1.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	b/h/p/d.java b/h/b.java b/h/n/c.java b/h/k/g.java b/h/j/c/q.java b/h/k/i.java b/h/r/j0.java b/n/a/b.java b/h/k/o.java g/b/a/h.java b/h/r/l.java b/k/a/b.java g/b/a/m/c.java b/h/q/b.java b/h/j/c/b.java b/h/k/d.java b/h/k/h.java g/b/a/c.java g/b/a/b.java g/b/a/m/h.java b/h/j/c/n.java org/acra/g/b.java b/h/r/j.java c/a/a/b/p/b.java b/b/o/j.java g/b/a/m/j.java b/f/b/q/j.java b/p/b1.java g/b/a/m/f.java c/a/a/b/m/h.java b/q/a/a/u.java b/f/b/g.java b/h/r/d1/c.java c/a/a/b/z/g.java b/h/r/u0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/l/b.java org/emunix/unipatcher/patcher/h.java org/emunix/unipatcher/l/j.java org/emunix/unipatcher/d.java
4	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
5	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/acra/file/Directory.java
6	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	g/b/a/f.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.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	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/armeabi-v7a/liblzma.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
3	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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/x86/liblzma.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
5	lib/arm64-v8a/libxdelta3.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	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
6	lib/arm64-v8a/liblzma.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
7	lib/x86_64/libxdelta3.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	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
8	lib/x86_64/liblzma.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	IDENTIFIER	REQUIREMENT	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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
schemas.android.com	ok	No Geolocation information available.
hosted.weblate.org	ok	**IP:** 116.203.108.97 **Country:** Germany **Region:** Bayern **City:** Gunzenhausen **Latitude:** 48.323330 **Longitude:** 11.601220 **View:** Google Map
play.google.com	ok	**IP:** 142.251.36.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
commons.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.paypal.com	ok	**IP:** 23.0.250.159 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
materialdesignicons.com	ok	**IP:** 34.234.179.93 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

EMAILS

EMAIL	FILE
unipatcher@gmail.com	org/emunix/unipatcher/UniPatcher.java
btimofeev@emunix.org	org/emunix/unipatcher/ui/activity/DonateActivity.java
unipatcher@gmail.com	Android String Resource

HARDCODED SECRETS

POSSIBLE SECRETS
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"

POSSIBLE SECRETS
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "بيتكوين"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Биткоин"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"

POSSIBLE SECRETS
"donations__bitcoin" : "„Bitcoin“"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "比特币"
"donations__bitcoin_send_bitcoin_button" : "发送比特币！"
"donations__bitcoin_toast_copy" : "比特币地址已被复制到剪贴板！"
"donations__bitcoin" : "比特幣"
"donations__bitcoin_description" : "將任意數量的比特幣發送給開發人。按住按鈕複製地址。"
"donations__bitcoin_send_bitcoin_button" : "發送比特幣！"
"donations__bitcoin_toast_copy" : "比特幣地址已被複製到剪貼板！"
"donations__bitcoin" : "Bitcoin"

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.