**Name of JNI file**: libfoo.so

**Package Name**: owasp.mstg.uncrackable2

**Native libs**

* Arch list: arm64-v8a, armeabi-v7a, x86, x86\_64
* Per arch count: arm64-v8a:1, armeabi-v7a:1, x86:1, x86\_64:1
* Total count: 4
* lib/arm64-v8a/libfoo.so
* lib/armeabi-v7a/libfoo.so
* lib/x86/libfoo.so
* lib/x86\_64/libfoo.so

### APK Signature v1: Signer CERT.RSA (META-INF/CERT.SF)

Type: X.509

Version: 3

Serial number: 0x71861047

Subject: CN=Jeroen Willemsen, OU=OMTG, O=OWASP, L=Amsterdam, C=NL

Valid from: Tue Aug 28 02:31:01 IST 2018

Valid until: Sat Aug 22 02:31:01 IST 2043

Public key type: RSA

Exponent: 65537

Modulus size (bits): 2048

Modulus: 17015576572051765181486540017741044803721108557364183786053756086523278332885423198276385730642416681952257865361476702646583356846951787236118011313986209229357938207404357857713536045442533175606742390875607905061375823188731453375834710432486645279165741574127942081900784487960806678749446912002864074253694233504123733231520652332362275042219236845882106567831628080893764031136045267125912203573818127193756515778073016871079804660718116275630474260238406960572120737868632153503103729779014008322164898684625688205238707276257604460627590868848234478308014374047438813813491305230122711169002966591350232063997

Signature type: SHA256withRSA

Signature OID: 1.2.840.113549.1.1.11

MD5 Fingerprint: 10 61 E3 C4 90 01 FC C5 F0 79 32 52 78 DF 94 CA

SHA-1 Fingerprint: 13 E4 9A 39 E6 28 81 7C BB DE 28 81 F4 64 6C 2A 0B 22 AD B2

SHA-256 Fingerprint: CB E6 8A B8 7D 64 34 1C 3F C7 81 19 DC 12 29 E8 AA 86 F9 3F DB 2C 33 AA 61 25 2F D4 91 48 5B 1D

**APK Signature v2:**

### Signer 1

Type: X.509

Version: 3

Serial number: 0x71861047

Subject: CN=Jeroen Willemsen, OU=OMTG, O=OWASP, L=Amsterdam, C=NL

Valid from: Tue Aug 28 02:31:01 IST 2018

Valid until: Sat Aug 22 02:31:01 IST 2043

Public key type: RSA

Exponent: 65537

Modulus size (bits): 2048

Modulus: 17015576572051765181486540017741044803721108557364183786053756086523278332885423198276385730642416681952257865361476702646583356846951787236118011313986209229357938207404357857713536045442533175606742390875607905061375823188731453375834710432486645279165741574127942081900784487960806678749446912002864074253694233504123733231520652332362275042219236845882106567831628080893764031136045267125912203573818127193756515778073016871079804660718116275630474260238406960572120737868632153503103729779014008322164898684625688205238707276257604460627590868848234478308014374047438813813491305230122711169002966591350232063997

Signature type: SHA256withRSA

Signature OID: 1.2.840.113549.1.1.11

MD5 Fingerprint: 10 61 E3 C4 90 01 FC C5 F0 79 32 52 78 DF 94 CA

SHA-1 Fingerprint: 13 E4 9A 39 E6 28 81 7C BB DE 28 81 F4 64 6C 2A 0B 22 AD B2

SHA-256 Fingerprint: CB E6 8A B8 7D 64 34 1C 3F C7 81 19 DC 12 29 E8 AA 86 F9 3F DB 2C 33 AA 61 25 2F D4 91 48 5B 1D

**JNI library files:**

**Comparison function:**

int strncmp(char \*\_\_s1,char \*\_\_s2,size\_t \_\_n)

{

int iVar1;

iVar1 = strncmp(\_\_s1,\_\_s2,\_\_n);

return iVar1;

}

**Codecheck function :**

void Java\_sg\_vantagepoint\_uncrackable2\_CodeCheck\_bar

(long \*param\_1,undefined8 param\_2,undefined8 param\_3)

{

long lVar1;

int iVar2;

undefined8 uVar3;

char \*\_\_s1;

undefined8 local\_50;

undefined8 uStack\_48;

undefined8 local\_40;

long local\_38;

lVar1 = tpidr\_el0;

local\_38 = \*(long \*)(lVar1 + 0x28);

uVar3 = 0;

if (DAT\_0011300c == '\x01') {

uStack\_48 = 0x74206c6c6120726f;

local\_50 = 0x6620736b6e616854;

local\_40 = 0x68736966206568;

\_\_s1 = (char \*)(\*\*(code \*\*)(\*param\_1 + 0x5c0))(param\_1,param\_3,0);

iVar2 = (\*\*(code \*\*)(\*param\_1 + 0x558))(param\_1,param\_3);

if ((iVar2 == 0x17) && (iVar2 = strncmp(\_\_s1,(char \*)&local\_50,0x17), iVar2 == 0)) {

uVar3 = 1;

}

else {

uVar3 = 0;

}

}

if (\*(long \*)(lVar1 + 0x28) == local\_38) {

return;

}

/\* WARNING: Subroutine does not return \*/

\_\_stack\_chk\_fail(uVar3);

}

**Mainactivity function:**

void Java\_sg\_vantagepoint\_uncrackable2\_MainActivity\_init(void)

{

FUN\_00100918();

DAT\_0011300c = 1;

return;

}

void FUN\_00100918(void)

{

long lVar1;

uint uVar2;

uint uVar3;

ulong uVar4;

pthread\_t local\_30;

long local\_28;

lVar1 = tpidr\_el0;

local\_28 = \*(long \*)(lVar1 + 0x28);

DAT\_00113008 = fork();

if (DAT\_00113008 == 0) {

uVar2 = getppid();

uVar4 = ptrace(PTRACE\_ATTACH,(ulong)uVar2,0,0);

if (uVar4 == 0) {

waitpid(uVar2,(int \*)&local\_30,0);

while( true ) {

ptrace(PTRACE\_CONT,(ulong)uVar2,0,0);

uVar3 = waitpid(uVar2,(int \*)&local\_30,0);

uVar4 = (ulong)uVar3;

if (uVar3 == 0) break;

if ((~(uint)local\_30 & 0x7f) != 0) {

/\* WARNING: Subroutine does not return \*/

\_exit(0);

}

}

}

}

else {

uVar2 = pthread\_create(&local\_30,(pthread\_attr\_t \*)0x0,FUN\_001008dc,(void \*)0x0);

uVar4 = (ulong)uVar2;

}

if (\*(long \*)(lVar1 + 0x28) == local\_28) {

return;

}

/\* WARNIN G: Subroutine does not return \*/

\_\_stack\_chk\_fail(uVar4);

}

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| DEFINED | 001004f9 |  | utf8 u8"\_\_cxa\_finalize" | "\_\_cxa\_finalize" | string | 15 | true |
| DEFINED | 00100508 |  | utf8 u8"\_\_cxa\_atexit" | "\_\_cxa\_atexit" | string | 13 | true |
| DEFINED | 00100515 |  | utf8 u8"Java\_sg\_vantagepoint\_uncrackable2\_CodeCheck\_bar" | "Java\_sg\_vantagepoint\_uncrackable2\_CodeCheck\_bar" | string | 48 | true |
| DEFINED | 00100545 |  | utf8 u8"Java\_sg\_vantagepoint\_uncrackable2\_MainActivity\_init" | "Java\_sg\_vantagepoint\_uncrackable2\_MainActivity\_init" | string | 52 | true |
| DEFINED | 00100579 |  | utf8 u8"\_\_stack\_chk\_fail" | "\_\_stack\_chk\_fail" | string | 17 | true |
| DEFINED | 0010058f |  | utf8 u8"getppid" | "getppid" | string | 8 | true |
| DEFINED | 00100597 |  | utf8 u8"pthread\_create" | "pthread\_create" | string | 15 | true |
| DEFINED | 001005a6 |  | utf8 u8"pthread\_exit" | "pthread\_exit" | string | 13 | true |
| DEFINED | 001005b3 |  | utf8 u8"ptrace" | "ptrace" | string | 7 | true |
| DEFINED | 001005ba |  | utf8 u8"strncmp" | "strncmp" | string | 8 | false |
| DEFINED | 001005c2 |  | utf8 u8"waitpid" | "waitpid" | string | 8 | true |
| DEFINED | 001005ca |  | utf8 u8"libm.so" | "libm.so" | string | 8 | false |
| DEFINED | 001005d2 |  | utf8 u8"libdl.so" | "libdl.so" | string | 9 | false |
| DEFINED | 001005db |  | utf8 u8"libc.so" | "libc.so" | string | 8 | false |
| DEFINED | 001005e3 |  | utf8 u8"\_edata" | "\_edata" | string | 7 | true |
| DEFINED | 001005ea |  | utf8 u8"\_\_bss\_start" | "\_\_bss\_start" | string | 12 | true |
| DEFINED | 001005f6 |  | utf8 u8"\_\_bss\_start\_\_" | "\_\_bss\_start\_\_" | string | 14 | true |
| DEFINED | 00100604 |  | utf8 u8"\_\_bss\_end\_\_" | "\_\_bss\_end\_\_" | string | 12 | true |
| DEFINED | 00100610 |  | utf8 u8"\_\_end\_\_" | "\_\_end\_\_" | string | 8 | true |
| DEFINED | 0010061d |  | utf8 u8"libfoo.so" | "libfoo.so" | string | 10 | true |
| DEFINED | 00101dec |  | ds "Android" (ElfNote\_8\_132.name) | "Android" | string | 8 | true |
| CONFLICTS | 00101e38 |  | db 35h (byte[132]description[68]) | "5063045" | string | 8 | false |