NULL Pointer Dereference in function mobi_build_opf_metadata at opf.c:1161 in bfabiszewski/libmobi

0

Valid Reported on Apr 26th 2022

Description

NULL Pointer Dereference in function mobi_build_opf_metadata at opf.c:1161 allows attackers to cause a denial of service (application crash) via a crafted input file

Build

```
git clone https://github.com/bfabiszewski/libmobi.git
cd libmobi

export CFLAGS="-g -O0 -lpthread -fsanitize=address"
export CXXFLAGS="-g -O0 -lpthread -fsanitize=address"
export LDFLAGS="-fsanitize=address"

./autogen.sh

./configure --disable-shared

make
```

POC

```
./tools/mobitool -e -o ./tmp/ ./poc_n.mobi

Title: libmobi ncx test
Publishing date: 2018-08-07
Language: en (utf8)
```

```
Dictionary

__
Mobi version: 1 (hybrid with version 6)

Creator software: kindlegen 2.9.0 (mac)

Reconstructing source resources...
AddressSanitizer:DEADLYSIGNAL
=================================================================
==3686533==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000
==3686533==The signal is caused by a READ memory access.
==3686533==Hint: address points to the zero page.
    #0 0x7ffff7bde5f5  /build/glibc-sMfBJT/glibc-2.31/string/../sysdeps/x86
    #1 0x483442 in strdup (/home/fuzz/libmobi/tools/mobitool+0x483442)
    #2 0x554adf in mobi_build_opf_metadata /home/fuzz/libmobi/src/opf.c:116
    #3 0x55e2a3 in mobi_build_opf /home/fuzz/libmobi/src/opf.c:1901:20
    #4 0x501166 in mobi_parse_rawml_opt /home/fuzz/libmobi/src/parse_rawml.
    #5 0x4ff78f in mobi_parse_rawml /home/fuzz/libmobi/src/parse_rawml.c:20
    #6 0x4c98d4 in loadfilename /home/fuzz/libmobi/tools/mobitool.c:852:20
    #7 0x4c8b36 in main /home/fuzz/libmobi/tools/mobitool.c:1051:11
    #8 0x7ffff7a7a0b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/c
    #9 0x41d57d in _start (/home/fuzz/libmobi/tools/mobitool+0x41d57d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /build/glibc-sMfBJT/glibc-2.31/string/../sy
==3686533==ABORTING
```

poc_n.mobi

GDB

```
Breakpoint 1, mobi_build_opf_metadata (opf=0x7fffffffc6c0, m=0x607000000100
1161                    opf->metadata->x_meta->dictionary_in_lang[0] = strd
─── Assembly ──────────────────────────────────────────────────────────────
 0x0000000000554ab2  mobi_build_opf_metadata+12530 mov    0x168(%rbx),%rdi
 0x0000000000554ab9  mobi_build_opf_metadata+12537 callq  0x
 0x0000000000554abe  mobi_build_opf_metadata+12542 mov    0x
 0x0000000000554ac5  mobi_build_opf_metadata+12549 mov    (%rax),%ecx
```

```
 0x0000000000554ac7  mobi_build_opf_metadata+12551 mov    %ecx,0x680(%rbx)
!0x0000000000554acd  mobi_build_opf_metadata+12557 mov    0x680(%rbx),%edi
 0x0000000000554ad3  mobi_build_opf_metadata+12563 callq  0x5158a0 <mobi_ge

 0x0000000000554ad8  mobi_build_opf_metadata+12568 mov    %rax,%rdi
 0x0000000000554adb  mobi_build_opf_metadata+12571 callq  0x483400 <strdup>
 0x0000000000554ae0  mobi_build_opf_metadata+12576 mov    0x6d0(%rbx),%rdx
── Breakpoints ──────────────────────────────────────────────────────────────
[1] break at 0x0000000000554acd in opf.c:1161 for opf.c:1161 hit 1 time
── Expressions ──────────────────────────────────────────────────────────────
── History ──────────────────────────────────────────────────────────────────
── Memory ───────────────────────────────────────────────────────────────────
── Registers ────────────────────────────────────────────────────────────────
    rax 0x0000602000000ef0     rbx 0x00007fffffffbfa0     rcx 0x0000000000
     r9 0x0000000000000002     r10 0x0000000000000040     r11 0x0000000000
     cs 0x00000033              ss 0x0000002b              ds 0x00000000
── Source ───────────────────────────────────────────────────────────────────
 1156                 if (opf->metadata->x_meta->dictionary_in_lang == NUL
 1157                     debug_print("%s\n", "Memory allocation failed");
 1158                     return MOBI_MALLOC_FAILED;
 1159                 }
 1160                 uint32_t dict_lang_in = *m->mh->dict_input_lang;
!1161                 opf->metadata->x_meta->dictionary_in_lang[0] = strdu
 1162             }
 1163         }
 1164         if (opf->metadata->x_meta->dictionary_out_lang == NULL) {
 1165             if (m->mh && m->mh->dict_output_lang) {
── Stack ────────────────────────────────────────────────────────────────────
[0] from 0x0000000000554acd in mobi_build_opf_metadata+12557 at opf.c:1161
[1] from 0x000000000055e2a4 in mobi_build_opf+436 at opf.c:1901
[2] from 0x0000000000501167 in mobi_parse_rawml_opt+6599 at parse_rawml.c:2
[3] from 0x00000000004ff790 in mobi_parse_rawml+96 at parse_rawml.c:2005
[4] from 0x00000000004c98d5 in loadfilename+2613 at mobitool.c:852
[5] from 0x00000000004c8b37 in main+5959 at mobitool.c:1051
── Threads ──────────────────────────────────────────────────────────────────
[1] id 3795174 name mobitool from 0x0000000000554acd in mobi_build_opf_meta
── Variables ────────────────────────────────────────────────────────────────
arg opf = 0x7fffffffc6c0: {metadata = 0x603000000e50,manifest = 0x0,spine =
loc dict_lang_in = 8323072
──────────────────────────────────────────────────────────────────────────────
>>> p mobi_get_locale_string(dict_lang_in)
$1 = 0x0
```

```
$1 = 0x0
```

Impact

NULL Pointer Dereference in function mobi_build_opf_metadata at opf.c:1161 allows attackers to cause a denial of service (application crash) via a crafted input file

Occurrences

C opf.c L1161

Call strdup with NULL pointer: strdup(NULL)

CVE
CVE-2022-2279
(Published)

Vulnerability Type
CWE-476: NULL Pointer Dereference

Severity
Medium (6.6)

Registry
Other

Affected Version
*

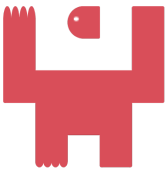
Visibility
Public

Status
Fixed

Found by

TDHX ICS Security
@jieyongma
pro

Fixed by



Bartek Fabiszewski

@bfabiszewski

unranked

This report was seen 511 times.

We are processing your report and will contact the **bfabiszewski/libmobi** team within 24 hours.
7 months ago

We have contacted a member of the **bfabiszewski/libmobi** team and are waiting to hear back
7 months ago

We have sent a follow up to the **bfabiszewski/libmobi** team. We will try again in 7 days.
7 months ago

Bartek 7 months ago Maintainer

Thanks for another report

Bartek Fabiszewski validated this vulnerability 7 months ago

TDHX ICS Security has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bartek Fabiszewski marked this as fixed in **0.11** with commit **c0699c** 7 months ago

Bartek Fabiszewski has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

opf.c#L1161 has been validated ✔

TDHX 5 months ago Researcher

@admin can we get a CVE for this?

Jamie Slome 5 months ago Admin

Sure, happy to assign and publish a CVE with the permission of the maintainer.

@Bartek - are you happy for me to assign and publish a CVE for this report?

Bartek 5 months ago Maintainer

@admin Yes! Thanks!

Jamie Slome 5 months ago Admin

Sorted!

Sign in to join this conversation