heap-buffer-overflow in mobi_get_attribute_value in bfabiszewski/libmobi

0

Valid Reported on Apr 30th 2022

Description

heap-buffer-overflow /home/ubuntu/libmobi-public/src/parse_rawml.c:357 in mobi_get_attribute_value

Environment

```
Distributor ID: Ubuntu
Description:    Ubuntu 20.04 LTS
Release:    20.04
Codename:   focal
mobitool build: Apr 29 2022 20:52:30 (gcc 9.3.0)
libmobi: 0.10
```

Build

```
export CC=gcc CXX=g++ CFLAGS="-fsanitize=address -static-libasan" CXXFLAGS=
autogen.sh &&  ./configure && make
```

POC

```
./mobitool -e -o ./tmp/ ./poc4
```

poc4

ASAN

ASAN

```
=================================================================
==150005==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61b000
READ of size 1 at 0x61b00000141f thread T0
    #0 0x55dae390a640 in mobi_get_attribute_value /home/ubuntu/libmobi-publ
    #1 0x55dae391760d in mobi_get_filepos_array /home/ubuntu/libmobi-public
    #2 0x55dae391760d in mobi_reconstruct_links_kf7 /home/ubuntu/libmobi-pu
    #3 0x55dae391b0d0 in mobi_reconstruct_links /home/ubuntu/libmobi-public
    #4 0x55dae391b0d0 in mobi_parse_rawml_opt /home/ubuntu/libmobi-public/s
    #5 0x55dae391b0d0 in mobi_parse_rawml /home/ubuntu/libmobi-public/src/p
    #6 0x55dae37bee00 in loadfilename /home/ubuntu/libmobi-public/tools/mob
    #7 0x55dae37bee00 in main /home/ubuntu/libmobi-public/tools/mobitool.c:
    #8 0x7feb6690f0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6
    #9 0x55dae37ca6fd in _start (/home/ubuntu/libmobi-public/tools/mobitool

0x61b00000141f is located 0 bytes to the right of 1439-byte region [0x61b00
allocated by thread T0 here:
    #0 0x55dae38b5748 in malloc (/home/ubuntu/libmobi-public/tools/mobitool
    #1 0x55dae390ffc0 in mobi_reconstruct_parts /home/ubuntu/libmobi-public

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/ubuntu/libmobi-public
Shadow bytes around the buggy address:
  0x0c367fff8230: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c367fff8240: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c367fff8250: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c367fff8260: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c367fff8270: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c367fff8280: 00 00 00[07]fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c367fff8290: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c367fff82a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c367fff82b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c367fff82c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c367fff82d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
```

```
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==150005==ABORTING
```

Impact

The bug causes the program reads data past the end of the intented buffer. Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash.

Occurrences

C parse_rawml.c L357

CVE
CVE-2022-1907
(Published)

Vulnerability Type
CWE-126: Buffer Over-read

Severity
Low (3.6)

Registry
Other

Affected Version

0.10

Visibility
Public

Status
Fixed

Found by

cnitlrt
@cnitlrt
master

Fixed by

Bartek Fabiszewski
@bfabiszewski
unranked

This report was seen 521 times.

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

cnitlrt modified the report 7 months ago

cnitlrt modified the report 7 months ago

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

Bartek Fabiszewski modified the CWE from Heap-based Buffer Overflow to Buffer Over-read 7 months ago

Bartek Fabiszewski modified the Severity from High (7.9) to Low (3.6) 7 months ago

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

The researcher has received a minor penalty to their credibility for misclassi
vulnerability type: -1

Bartek Fabiszewski validated this vulnerability 7 months ago

cnitlrt has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +5

Bartek Fabiszewski marked this as fixed in 0.11 with commit 1e0378 7 months ago

Bartek Fabiszewski has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

parse_rawml.c#L357 has been validated ✔

Bartek 7 months ago Maintainer

Thanks for finding this bug!

cnitlrt 6 months ago Researcher

@Bartek @admin Can i request the cve for this report and another report?

Jamie Slome 6 months ago Admin

@Bartek - if you give me the go-ahead, I can assign and publish CVEs for both reports 👍

Bartek 6 months ago Maintainer

Please, go ahead with CVEs.
Thanks!

cnitlrt 6 months ago Researcher

Thanks!

Sign in to join this conversation

Chat with us