kevinboone / epub2txt2 Public

Code Issues 1 Pull requests 1 Actions Projects Security ...

New issue

Jump to bottom

[Bug Report]stack-buffer-overflow in Function epub2txt_do_file() AT src/epub2txt.c #17

Closed Asteriska8 opened this issue on Jan 22 · 4 comments

Asteriska8 commented on Jan 22

Description

A stack-buffer-overflow was discovered in epub2txt2.
The issue is being triggered in function xhtml_translate_entity() at src/xhtml.c:576

Version

Version 2.02 (Lastest)

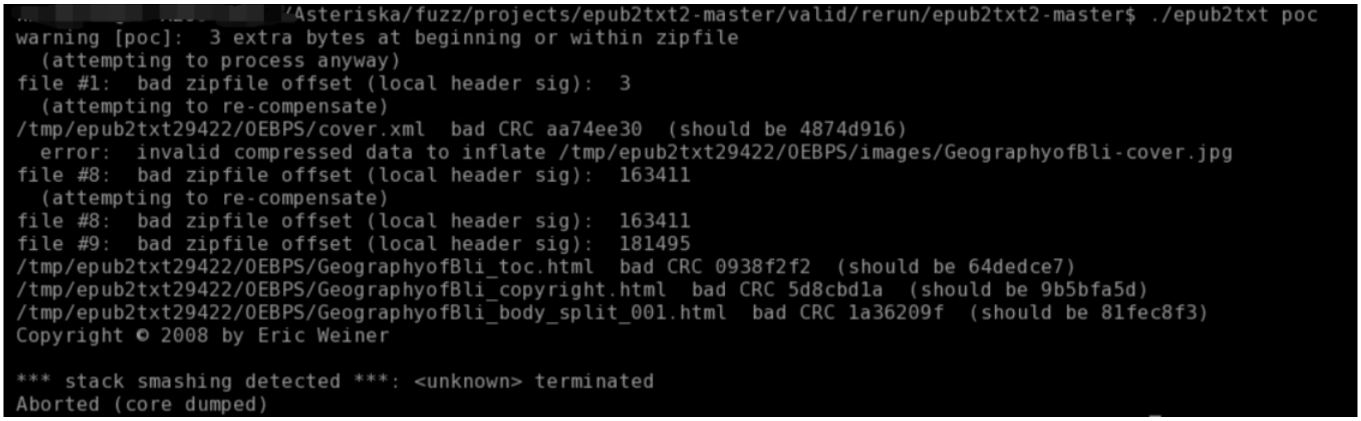
Environment

Ubuntu 18.04, 64bit

Reproduce

Command

```
git clone the Lastest Version firstly.
make && make install
./epub2txt poc
```



```
[redacted]/Asteriska/fuzz/projects/epub2txt2-master/valid/rerun/epub2txt2-master$ ./epub2txt poc
warning [poc]:  3 extra bytes at beginning or within zipfile
  (attempting to process anyway)
file #1:  bad zipfile offset (local header sig):  3
  (attempting to re-compensate)
/tmp/epub2txt29422/OEBPS/cover.xml  bad CRC aa74ee30  (should be 4874d916)
  error:  invalid compressed data to inflate /tmp/epub2txt29422/OEBPS/images/GeographyofBli-cover.jpg
file #8:  bad zipfile offset (local header sig):  163411
  (attempting to re-compensate)
file #8:  bad zipfile offset (local header sig):  163411
file #9:  bad zipfile offset (local header sig):  181495
/tmp/epub2txt29422/OEBPS/GeographyofBli_toc.html  bad CRC 0938f2f2  (should be 64dedce7)
/tmp/epub2txt29422/OEBPS/GeographyofBli_copyright.html  bad CRC 5d8cbd1a  (should be 9b5bfa5d)
/tmp/epub2txt29422/OEBPS/GeographyofBli_body_split_001.html  bad CRC 1a36209f  (should be 81fec8f3)
Copyright © 2008 by Eric Weiner

*** stack smashing detected ***: <unknown> terminated
Aborted (core dumped)
```

POC file at the bottom of this report.

With ASAN

Note: You can use ASAN for more direct verification.

```
Compile program with address sanitizer with this command:
VERSION := 2.02
CC      := gcc
CFLAGS  := -Wall -fPIC -fPIE
LDLAGS  := -pie
DESTDIR :=
PREFIX  := /usr
BINDIR  := /bin
MANDIR  := /share/man
APPNAME := epub2txt

TARGET  := epub2txt
SOURCES := $(shell find src/ -type f -name *.c)
OBJECTS := $(patsubst src/%,build/%,$(SOURCES:.c=.o))
DEPS    := $(OBJECTS:.o=.deps)

$(TARGET): $(OBJECTS)
        $(CC) -fsanitize=address -o $(TARGET) $(LDFLAGS) $(OBJECTS)

build/%.o: src/%.c
        @mkdir -p build/
        $(CC) $(CFLAGS) -fsanitize=address -g -DVERSION=\"$(VERSION)\" -DAPPNAME=\"$(APPNAME)\" -
MD -MF $(@:.o=.deps) -c -o $@ $<

clean:
        $(RM) -r build/ $(TARGET)

install:
        install -D -m 755 $(APPNAME) $(DESTDIR)/$(PREFIX)/$(BINDIR)/$(APPNAME)
        install -D -m 644 man1/epub2txt.1 $(DESTDIR)/$(PREFIX)/$(MANDIR)/man1/epub2txt.1

uninstall:
        rm -f $(DESTDIR)/$(PREFIX)/$(BINDIR)/$(APPNAME)
        rm -f $(DESTDIR)/$(PREFIX)/$(MANDIR)/man1/epub2txt.1
```

```
-include $(DEPS)

.PHONY: clean install
```

ASAN Report

```
warning [./input/id:000029,sig:11,src:000553,time:174169875,op:havoc,rep:4]:  3 extra bytes at beginning or within zipfile
  (attempting to process anyway)
file #1:  bad zipfile offset (local header sig):  3
  (attempting to re-compensate)
/tmp/epub2txt14993/OEBPS/cover.xml  bad CRC aa74ee30  (should be 4874d916)
  error:  invalid compressed data to inflate /tmp/epub2txt14993/OEBPS/images/GeographyofBli-cover.jpg
file #8:  bad zipfile offset (local header sig):  163411
  (attempting to re-compensate)
file #8:  bad zipfile offset (local header sig):  163411
file #9:  bad zipfile offset (local header sig):  181495
/tmp/epub2txt14993/OEBPS/GeographyofBli_toc.html  bad CRC 0938f2f2  (should be 64dedce7)
/tmp/epub2txt14993/OEBPS/GeographyofBli_copyright.html  bad CRC 5d8cbd1a  (should be 9b5bfa5d)
/tmp/epub2txt14993/OEBPS/GeographyofBli_body_split_001.html  bad CRC 1a36209f  (should be 81fec8f3)
=================================================================
==14993==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7fffffffcb14 at pc 0x7ffff6e7e3a6 bp 0x7fffffffca60 sp 0x7fffffffc208
WRITE of size 305 at 0x7fffffffcb14 thread T0
    #0 0x7ffff6e7e3a5  (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x663a5)
    #1 0x55555558000e in xhtml_translate_entity src/xhtml.c:576
    #2 0x555555580b34 in xhtml_to_stdout src/xhtml.c:789
    #3 0x555555580680 in xhtml_file_to_stdout src/xhtml.c:700
    #4 0x555555560476 in epub2txt_do_file src/epub2txt.c:494
    #5 0x55555555d3c9 in main src/main.c:187
    #6 0x7ffff6a48bf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
    #7 0x55555555c219 in _start (/home/nisl1/nisl8121/Asteriska/fuzz/projects/epub2txt2-master/valid/epub2txt+0x8219)

Address 0x7fffffffcb14 is located in stack of thread T0 at offset 116 in frame
    #0 0x55555557fad4 in xhtml_translate_entity src/xhtml.c:532

  This frame has 2 object(s):
    [32, 36) 'v'
    [96, 116) 'out' <== Memory access at offset 116 overflows this variable
HINT: this may be a false positive if your program uses some custom stack unwind mechanism or swapcontext
      (longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-buffer-overflow (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x663a5)
Shadow bytes around the buggy address:
  0x10007fff7910: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007fff7920: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007fff7930: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007fff7940: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007fff7950: 00 00 00 00 f1 f1 f1 f1 04 f2 f2 f2 f2 f2 f2 f2
=>0x10007fff7960: 00 00[04]f2 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007fff7970: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007fff7980: 00 00 f1 f1 f1 f1 f8 f2 f2 f2 00 00 00 00 00 00
  0x10007fff7990: 00 00 00 00 00 00 00 00 f1 f1 f1 f1 00 f2 f2 f2
  0x10007fff79a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007fff79b0: 00 00 00 00 00 00 f1 f1 f1 f1 f8 f2 f2 f2 f2 f2
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
==14993==ABORTING
```

POC

POC

Any issue plz contact with me:
admin@hack.best
OR:
twitter: **@Asteriska8**

Mohad0 mentioned this issue on Jan 23

nvm #18

Closed

kevinboone commented on Jan 24 Owner

I'm unsure what work is required here. I'm not remotely surprised that epub2txt is prone to buffer-overrun situations, but I'm not sure what the significance is. This isn't a utility that's going to be run unattended as a server process, so I don't see how these buffer-overruns are exploitable in any practical way. If I have misunderstood, feel free to correct me.

Asteriska8 commented on Jan 25 Author

> I'm unsure what work is required here. I'm not remotely surprised that epub2txt is prone to buffer-overrun situations, but I'm not sure what the significance is. This isn't a utility that's going to be run unattended as a server process, so I don't see how these buffer-overruns are exploitable in any practical way. If I have misunderstood, feel free to correct me.

Hi Kevin,
The epub2txt2 is a great utility so that it enjoys the popularity and is already available for a number of Linux distributions, with a number of users' employment.
And this vulnerability allows a stack-based buffer overflow via a crafted EPUB document, and if the attacker spread some crafted or poisoned EPUB documents that could do harm to the system to the internet or the victim's computer,so it's risky.

kevinboone commented on Jan 25 Owner

Thank you for reporting this problem. I had carelessly assumed that all XHTML documents in an EPUB would be well-formed. I had used a strcpy() call into a buffer of fixed length. I believe this is fixed in the latest push -- please let me know if you think otherwise.

Asteriska8 commented on Jan 25 Author

Nice work :). This vulnerability was fixed.
Thanks.

Asteriska8 closed this as completed on Jan 25

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants