Stack out-of-bounds read in gif_get_code() #463

Closed **Jorgecmartins** opened this issue on Jan 7 · 5 comments

Assignees	
Labels	bug platform issue priority-low
Milestone	Stable

Jorgecmartins commented on Jan 7 Contributor

In `gif_get_code()`, in image.cxx, there is a stack out-of-bounds read in the following code:

```
267   curbit    = (curbit - lastbit) + 8 * last_byte;
268   last_byte += (unsigned)count;
269   lastbit   = last_byte * 8;
270 }
271
272 for (ret = 0, i = curbit + (unsigned)code_size - 1, j = (unsigned)code_size;
273      j > 0;
274      i --, j --)
275   ret = (ret << 1) | ((buf[i / 8] & bits[i & 7]) != 0);
```

The expression `curbit - lastbit`, line 267, can result in an integer overflow when `lastbit > curbit`, updating `curbit` to a large number since it is unsigned. Later on line 272 the variable `i` is set to number less than `code_size`, since `curbit + (unsigned)code_size - 1` overflows, which results after a few iterations in a stack out of bounds read in `buf[i/8]`.

I've attached poc.zip that contains a malicious gif and a html file and triggers the out of bounds read resulting in a segmentation fault.

Steps to reproduce

The following should result in a segmentation fault:

```
$ unzip poc.zip
$ htmldoc --webpage -f output.pdf crash.html
```

Steps to analyse the crash on gdb

```
gdb --args htmldoc --webpage -f output.pdf ./crash.html
# set a breakpoint on gif_get_code
run
continue 3
# reached the gif_get_code that will crash
```

michaelrsweet self-assigned this on Jan 7

michaelrsweet added unable-to-reproduce **bug** platform issue **priority-low** and removed unable-to-reproduce labels on Jan 7

michaelrsweet added this to the **Stable** milestone on Jan 7

michaelrsweet commented on Jan 7 Owner

@Jorgecmartins I've tried this on macOS and Linux (Ubuntu 20.04), but only Linux reproduces.

michaelrsweet commented on Jan 7 Owner

[master `776cf0f`] Fix potential stack overflow with GIF images (Issue #463)

michaelrsweet closed this as completed on Jan 7

michaelrsweet added a commit that referenced this issue on Jan 7

`Fix potential stack overflow with GIF images (Issue #463)` `776cf0f`

Jorgecmartins commented on Jan 7 Contributor Author

> **@Jorgecmartins** I've tried this on macOS and Linux (Ubuntu 20.04), but only Linux reproduces.

@michaelrsweet I was also able to reproduce it on macOS.

```
Jorge@MacBook-Pro-de-Jorge htmldoc % ./htmldoc --webpage -f output.pdf ./crash.html
ERR005: Unable to open psglyphs data file!
ERR005: Unable to open character set file iso-8859-1!
ERR005: Unable to open font width file /usr/local/share/htmldoc/fonts/Times-Roman.afm!
ERR005: Unable to open psglyphs data file!
ERR005: Unable to open character set file iso-8859-1!
ERR005: Unable to open psglyphs data file!
ERR005: Unable to open character set file iso-8859-1!
ERR005: Unable to open font width file /usr/local/share/htmldoc/fonts/Helvetica.afm!
ERR005: Unable to open font width file /usr/local/share/htmldoc/fonts/Helvetica.afm!
ERR005: Unable to open font width file /usr/local/share/htmldoc/fonts/Helvetica.afm!
ERR005: Unable to open font width file /usr/local/share/htmldoc/fonts/Helvetica.afm!
ERR005: Unable to open font width file /usr/local/share/htmldoc/fonts/Helvetica.afm!
ERR005: Unable to open font width file /usr/local/share/htmldoc/fonts/Helvetica.afm!
PAGES: 2
ERR005: Unable to open font file /usr/local/share/htmldoc/fonts/Helvetica.pfa!
zsh: segmentation fault  ./htmldoc --webpage -f output.pdf ./crash.html
```

macOS version: 11.6

```
Jorge@MacBook-Pro-de-Jorge htmldoc % uname -a
Darwin MacBook-Pro-de-Jorge.local 20.6.0 Darwin Kernel Version 20.6.0: Mon Aug 30 06:12:21 PDT
2021; root:xnu-7195.141.6~3/RELEASE_X86_64 x86_64
```

michaelrsweet added a commit that referenced this issue on Jan 7

`Block GIF images with a code size > 12 (Issue #463)` ✗ `312f0f9`

michaelrsweet commented on Jan 7 Owner

@Jorgecmartins I added another layer of protection here:

[master `312f0f9`] Block GIF images with a code size > 12 (Issue #463)

Jorgecmartins commented on Jan 10 Contributor Author

> **@Jorgecmartins** I added another layer of protection here:
>
> [master 312f0f9] Block GIF images with a code size > 12 (Issue #463)

@michaelrsweet The extra protection fixed the issue.

Assignees

michaelrsweet

Labels

bug platform issue priority-low

Projects

None yet

Milestone

Stable

Development

No branches or pull requests

2 participants