New issue

Jump to bottom

Bug: buffer-overflow caused by integer-overflow in image_load_gif() #423

Closed kangwoosukeq opened this issue on Mar 21, 2021 · 6 comments

Assignees

Labels bug priority-high

Milestone Stable

kangwoosukeq commented on Mar 21, 2021

Hi, I found some integer overflow vulnerability that is similar to CVE-2017-9181 in htmldoc.

- os : Debian GNU/Linux bullseye/sid
- version : 1.9.11

htmldoc-poc.zip
In htmldoc-poc, there are maliciously crafted gif and html file which crashes htmldoc like below.

```
$ htmldoc --webpage -f out.pdf htmldoc-poc.html
PAGES: 2
[1]    17884 segmentation fault  htmldoc --webpage -f out.pdf htmldoc-poc.html
```

The vulnerability resides in image_load_gif() function in htmldoc/image.cxx file.
In line 1279, the program reads data from given gif file using fread.

1279 fread(buf, 9, 1, fp);

Then, it stores value to 'img->width' and 'img->height' in line 1320,
and 'img->depth' is determined by whether given image is grayscale.

1320 img->width = (buf[5] << 8) | buf[4];
1321 img->height = (buf[7] << 8) | buf[6];
1322 img->depth = gray ? 1 : 3;

If load_data is equal to 1 and,
'img->width' and 'img->height' are enough large to cause an integer overflow,
the small heap block is allocated in line 1326.
It leads to buffer overrun when reads data to this buffer in gif_read_image().

1323 if (!load_data)
1324 return (0);
1325
1326 img->pixels = (uchar *)malloc((size_t)(img->width * img->height * img->depth));

michaelrsweet self-assigned this on Mar 22, 2021

michaelrsweet added the investigating label on Mar 22, 2021

michaelrsweet commented on Mar 22, 2021 Owner

Hmm, 65535 * 65535 should not cause an integer overflow on modern systems, but I'll happily limit GIF files to smaller sizes.

👍 1

michaelrsweet added a commit that referenced this issue on Mar 31, 2021

`Fix crash bug with bad GIFs (Issue #423)` ✕ 6a8322a

michaelrsweet commented on Mar 31, 2021 Owner

[master `6a8322a`] Fix crash bug with bad GIFs (Issue #423)

I added a range check to limit the width and height to 1-32767.

michaelrsweet closed this as completed on Mar 31, 2021

michaelrsweet added bug priority-high and removed investigating labels on Mar 31, 2021

michaelrsweet added this to the **Stable** milestone on Mar 31, 2021

carnil commented on Apr 6, 2021

This isse was assigned CVE-2021-20308

p.s.: is the CVE reference in the initial item correct? CVE-2017-9181 does not seem to be associated with htmldoc.

kangwoosukeq commented on Apr 6, 2021 Author

> This isse was assigned CVE-2021-20308
>
> p.s.: is the CVE reference in the initial item correct? CVE-2017-9181 does not seem to be associated with htmldoc.

I noticed it may confuse.

It means the bug type of this vulnerability and CVE-2017-9181 are similar.

Because they both cause integer overflow while multiplying the width and height of the input image, then lead to small heap block allocation & buffer overrun.

carnil commented on Apr 6, 2021

@kangwoosukeq thanks for clarification. I indeem might just have been confused about the wording "similar to CVE-2017-9181 in htmldoc". But now it's clear, you meant the class of issue/bug type.

michaelrsweet commented on Apr 6, 2021 Owner

@carnil @kangwoosukeq Well, the important thing is that it is fixed! :) As soon as I finish my final QA pass I'll be releasing an update of HTMLDOC...

emmanuelrosa mentioned this issue on May 4, 2021

Vulnerability roundup 101: htmldoc-1.8.29: 1 advisory [9.8] NixOS/nixpkgs#120384

Closed

1 task

kangwoosukeq mentioned this issue on Oct 7, 2021

Heap buffer overflow caused by an integer overflow #451

Closed

Assignees

michaelrsweet

Labels

bug priority-high

Projects

None yet

Milestone

Stable

Development

No branches or pull requests

3 participants