Redmine - Defect #26051

Please correct the vulnerability of imagemagick(CVE-2017-9098)

2017-05-27 08:45 - Sahya Norn

Status:	Closed	**Start date:**	
Priority:	High	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:	Wont fix	**Affected version:**	

Description

Please correct the vulnerability of imagemagick(CVE-2017-9098)

https://access.redhat.com/security/cve/cve-2017-9098

History

#1 - 2017-05-27 09:56 - Toshi MARUYAMA

How do you think we should do?

#2 - 2017-05-28 04:46 - Go MAEDA

Sahya, thank you for reporting this issue so quickly.

I think that Redmine 3.3.2 / 3.2.5 (released on 2017-01-07) and later are not affected with the vulnerability because they don't process Utah RLE images. By the change introduced in r16092, Redmine don't make ImageMagick process a image if the image format is not BMP, GIF, JPEG and PNG. But older versions of Redmine are vulnerable.

#3 - 2017-05-29 06:22 - Toshi MARUYAMA

On my CentOS7.

```
$ wget https://downloads.sourceforge.net/project/utahrastertoolkit/urt-img.tar
$ tar xf urt-img.tar
$ LC_ALL=C file img/christmas_ball.rle
img/christmas_ball.rle: RLE image data, 400 x 400, clear first, alpha channel, comment, 3 color channels, 8 bi
ts per pixel
$ sudo mv /usr/lib64/ImageMagick-6.7.8/modules-Q16/coders/rle.so /usr/lib64/ImageMagick-6.7.8/modules-Q16/code
rs/rle.so.CVE-2017-9098
$ convert img/christmas_ball.rle img/christmas_ball.png
convert: unable to load module `/usr/lib64/ImageMagick-6.7.8/modules-Q16/coders/rle.la': file not found @ erro
r/module.c/OpenModule/1278.
convert: no decode delegate for this image format `img/christmas_ball.rle' @ error/constitute.c/ReadImage/544.
convert: no images defined `img/christmas_ball.png' @ error/convert.c/ConvertImageCommand/3046.
$ echo $?
1
$ LC_ALL=C ls img/christmas_ball.png
ls: cannot access img/christmas_ball.png: No such file or directory
```

#4 - 2017-06-06 00:59 - Sahya Norn

> Toshi MARUYAMA wrote:
> How do you think we should do?

I think severity level of the vulnerability is high.
And any website is fixed.
I remember that Redmine use imagemagick.
So I reported this issue.

#5 - 2017-06-06 02:29 - Go MAEDA

- Status changed from New to Closed

- Resolution set to Wont fix

I think we can close this issue because current versions of Redmine (3.3.2 / 3.2.5 and later) don't treat Utah RLE files as images (r16092), therefore, they are not affected with the vulnerability.

Sahya, thank you for letting us know this serious vulnerability.