

New issue

[Jump to bottom](#)

Fix CVE 2022 41751 #57

Merged

Matthias-Wandel merged 2 commits into `Matthias-Wandel:master` from `kyle-tenet3:fix-CVE-2022-41751` on Oct 3

Conversation 0

Commits 2

Checks 0

Files changed 1

 kyle-tenet3 commented on Oct 3

Contributor

Hello, developers of jhead.

We have found an exploit that allows running an arbitrary shell command due to improper input validation ([CVE-20](#)). This pull request fixes this vulnerability.

Details

In the function `RegenerateThumbnail` in the file `jhead.c`, `system()` is called with a string that contains a user-provided filename, leaving it open to attack by using a crafted filename.

System Info

5.10.104-linuxkit: clang 10.0.0-4ubuntu1, gcc 9.4.0
jhead 3.06.0.1, commit [78057ab](#)

All testing was done in a Docker container, but this vulnerability should affect all platforms.

Verification

[Download test.jpeg](#).

This will work with any image with an EXIF thumbnail. The program [exiftran](#) can be used to add a thumbnail to an image that lacks one.

1. Download and compile:

```
wget https://github.com/Matthias-Wandel/jhead/archive/refs/tags/3.06.0.1.tar.gz
tar xzf 3.06.0.1.tar.gz
cd jhead-3.06.0.1
make
```

2. Copy a JPEG with an EXIF thumbnail to a filename that triggers the vulnerability:

```
cp path/to/test.jpeg 'test.jpeg"; exec "sh'
```

3. Run thumbnail regeneration to finish exploit:

```
./jhead -rgt50 'test.jpeg"; exec "sh'
sh: 1: mogrify: not found
$ ls
buildrpms      exifgaps.py      iptc.c  jhead.1  jhead.spec  make.bat      makernote.c
paths.c        rpmprep          tests
changes.txt    gpsinfo.c        iptc.h  jhead.c  jpgfile.c   makefile      myglob.c
read_write_notes.txt  test.jpeg        usage.html
exif.c         how-to-make-rpm.txt  jhead  jhead.h  jpgqguess.c  makefile-win32  obj
readme.txt     'test.jpeg"; exec "sh'
$
```

Whether the mogrify command exists does not affect the functioning of the exploit.

Fix

I added a check for certain characters in the filename in RegenerateThumbnail:

```
// Disallow characters in the filename that could be used to execute arbitrary
// shell commands with system() below.
if(strpbrk(FileName, "\";'&|`")) {
    ErrNonfatal("Filename has invalid characters.", 0, 0);
    return FALSE;
}
```

I also replaced a call to `sprintf` with `snprintf` in RegenerateThumbnail.




After applying the patch, files with invalid characters (such as quotes and other symbols with special meaning on the shell)


will be disallowed from being used in RegenerateThumbnail:

```
$ ./jhead -rgt50 'test.jpg"; exec "sh'
Nonfatal Error : 'test.jpg"; exec "sh' Filename has invalid characters.
```

A better solution would be to use a function such as `execve` on UNIX-based systems. I chose not to include this in the patch as it would complicate compilation on Windows-based systems, but it should also be possible to call a Windows API function such as `CreateProcess` or `ShellExecute` to run the command.

 **kyle-tenet3** added 2 commits 2 months ago

-   Replace `sprintf` with `snprintf` in `RegenerateThumbnail` 6985da5
-   Check for dangerous filenames in `RegenerateThumbnail` 3fe905c

 **Matthias-Wandel** merged commit **ba1da7d** into [Matthias-Wandel:master](#) on Oct 3

  **jwilk** mentioned this pull request on Oct 19

Incomplete fix for CVE-2022-41751 #60

 Open

Reviewers

No reviews

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

2 participants

