New issue

Jump to bottom

Uninitialized variable: mode in function im_vips2dz() #1419

Closed **yifengchen-cc** opened this issue on Sep 3, 2019 · 2 comments

Labels bug in development

yifengchen-cc commented on Sep 3, 2019

/libvips/libvips/deprecated/im_vips2dz.c:79
When the output file does not contain a ":", the uninitialization of the mode causes the stack information to leak.
This may cause the leakage of remote server path.

```
$./vips im_vips2dz /home/ivan/miniproject/libvips/tools/.libs/th.vips th.dz
im_vips2dz: enum 'VipsForeignDzLayout' has no member 'roject/libvips/tools/.libs/th.vips', should be one of: dz, zoomify, google
```

jcupitt commented on Sep 3, 2019 Member

Oh, good point! Thank you for reporting this. I've fixed git master.

The stuff in "deprecated" is not checked by the fuzzer :(

jcupitt added bug in development labels on Sep 3, 2019

jcupitt added a commit that referenced this issue on Sep 3, 2019

`fix a used-before-set error in im_vips2dz` ... 2ab5aa7

jcupitt closed this as completed on Sep 15, 2019

lovell commented on Nov 21, 2020 Member

It looks like this has been assigned CVE-2020-20739.

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-20739
https://nvd.nist.gov/vuln/detail/CVE-2020-20739

There's no severity listed, but I imagine usage in the wild of this deprecated code path will be very low.

Assignees
No one assigned

Labels
bug in development

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

3 participants