

# Code Injection vulnerability in CarrierWave::RMagick

Low

mshibuya published GHSA-cf3w-g86h-35x4 on Feb 7, 2021

Package

 carrierwave (RubyGems)

Affected versions

< 2.1.1 and < 1.3.2

Patched versions

2.1.1, 1.3.2

Description

Impact

CarrierWave::RMagick has a Code Injection vulnerability. Its #manipulate! method inappropriately evals the content of mutation option( :read / :write ), allowing attackers to craft a string that can be executed as a Ruby code.

If an application developer supplies untrusted inputs to the option, it will lead to remote code execution(RCE).

(But supplying untrusted input to the option itself is dangerous even in absence of this vulnerability, since is prone to DoS vulnerability - attackers can try to consume massive amounts of memory by resizing to a very large dimension)

Proof of Concept

```
class MyUploader < CarrierWave::Uploader::Base
  include CarrierWave::RMagick
end

MyUploader.new.manipulate!({ read: { density: "1 "; p 'Hacked'; {} }}) # => shows "Hacked"
```

Patches

Upgrade to 2.1.1 or 1.3.2.

Workarounds

Stop supplying untrusted input to #manipulate! 's mutation option.

References

[Code Injection Software Attack](#)

For more information

If you have any questions or comments about this advisory:

- Open an issue in [CarrierWave repo](#)
- Email me at [mit.shibuya@gmail.com](mailto:mit.shibuya@gmail.com)

Severity

Low


CVE ID

CVE-2021-21305

Weaknesses

No CWEs

Credits

 wonda-tea-coffee