Remote shell execution vulnerability in ImageProcessing

High janko published GHSA-cxf7-qrc5-9446 on Mar 1

Package

image_processing (RubyGems)

Affected versions

<= 1.12.1

Patched versions

1.12.2

Description

Impact

When using the `#apply` method from image_processing to apply a series of operations that are coming from unsanitized user input, this allows the attacker to execute shell commands:

```
ImageProcessing::Vips.apply({ system: "echo EXECUTED" })
#>> EXECUTED
```

This method is called internally by Active Storage variants, so Active Storage is vulnerable as well.

Patches

The vulnerability has been fixed in version 1.12.2 of image_processing.

Workarounds

If you're processing based on user input, it's highly recommended that you always sanitize the user input, by allowing only a constrained set of operations. For example:

```
operations = params[:operations]
  .map { |operation| [operation[:name], *operation[:value]] }
  .select { |name, *| name.to_s.include? %w[resize_to_limit strip ...] } # sanitization
```

```
    ImageProcessing::Vips.apply(operations)
```

Severity

High

CVE ID

CVE-2022-24720

Weaknesses

No CWEs