

## [CVE-2021-22902] Possible Denial of Service vulnerability in Action Dispatch

Aaron Patterson tenderlove core team

May '21

There is a possible Denial of Service vulnerability in the Mime type parser of Action Dispatch. This vulnerability has been assigned the CVE identifier CVE-2021-22902.

Versions Affected: >= 6.0.0 Not affected: < 6.0.0 Fixed Versions: 6.0.3.7, 6.1.0.2

### Impact

There is a possible Denial of Service vulnerability in Action Dispatch. Carefully crafted Accept headers can cause the mime type parser in Action Dispatch to do catastrophic backtracking in the regular expression engine.

### Releases

The fixed releases are available at the normal locations.

### Workarounds

The following monkey patch placed in an initializer can be used to work around the issue:

```
module Mime
  class Type
    MIME_REGEXP = /\A(?:\*\/*\#{MIME_NAME})\/(?:\*\#{MIME_NAME})(>\s*\#{MIME_P
    end
  end
end
```



### Patches



To aid users who aren't able to upgrade immediately we have provided patches for the two supported release series. They are in git-am format and consist of a single changeset.

- 6-0-Prevent-catastrophic-backtracking-during-mime-parsin.patch - Patch for 6.0 series
- 6-1-Prevent-catastrophic-backtracking-during-mime-parsin.patch - Patch for 6.1 series

Please note that only the 6.1.Z, 6.0.Z, and 5.2.Z series are supported at present. Users of earlier unsupported releases are advised to upgrade as soon as possible as we cannot guarantee the continued availability of security fixes for unsupported releases.

### Credits

Thanks to Security Curious [security-curious@pm.me](mailto:security-curious@pm.me) for reporting this!

 [6-1-Prevent-catastrophic-backtracking-during-mime-parsin.patch](#) (2.2 KB)  [6-0-Prevent-catastrophic-backtracking-during-mime-parsin.patch](#) (2.2 KB)

 More Resources

Keep up to date with [Rails on Twitter](#) and [This Week in Rails](#)

Policies: [Conduct](#), [License](#), [Maintenance](#), [Security](#), [Trademarks](#)