

## 9 `redirect_to(["string"])` remote code execution

Share:     

### SUMMARY BY RUBY ON RAILS



#### Impact

There is a possible information disclosure / unintended method execution vulnerability in Action Pack when using the `redirect_to` or `polymorphic_url` helper with untrusted user input.

Vulnerable code will look like this.

```
redirect_to(params[:some_param])
```

All users running an affected release should either upgrade or use one of the workarounds immediately.

#### Releases

The FIXED releases are available at the normal locations.

#### Workarounds

To work around this problem, it is recommended to use an allow list for valid parameters passed from the user. For example,

```
private def check(param)
  case param
  when "valid"
    param
  else
    "/"
  end
end
```

```
def index
  redirect_to(check(params[:some_param]))
end
```

Or force the user input to be cast to a string like this,

```
def index
  redirect_to(params[:some_param].to_s)
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.

5-2-information-disclosure.patch - Patch for 5.2 series

6-0-information-disclosure.patch - Patch for 6.0 series

6-1-information-disclosure.patch - Patch for 6.1 series

Please note that only the 5.2, 6.0, and 6.1 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 Benoit Côté-Jodoin from Shopify for reporting this.

#### References

<https://github.com/rails/rails/releases/tag/v5.2.4.6>

<https://github.com/rails/rails/releases/tag/v5.2.6>

<https://github.com/rails/rails/releases/tag/v6.0.3.7>

<https://github.com/rails/rails/releases/tag/v6.1.3.2>

<https://groups.google.com/g/rubyonrails-security/c/NiQI-48cXYI>

### TIMELINE



[gmcgibbon](#) submitted a report to [Ruby on Rails](#).

Feb 18th (2 years ago)

For example, `redirect_to(params[:user_input])` with a URL of `?user_input[]=something` calls the method `something_url` and tries to redirect the return value of the method. If this call is on an unauthenticated route, it would allow an external user to test if a route name exists by determining if the app 500s (the method does not exist) or successfully redirects.

#### Impact

Any public method defined on a controller ending with `_url` could be remotely executed.




[tenderlove](#) [Ruby on Rails staff](#) added weakness "Information Exposure Through an Error Message" and removed weakness "Code Injection".


Feb 23rd (2 years ago)





[tenderlove](#) [Ruby on Rails staff](#) updated CVE reference to [CVE-2021-22885](#).

Mar 9th (2 years ago)

-  [tenderlove](#) Ruby on Rails staff closed the report and changed the status to **Resolved**.

May 5th (2 years ago)
-  [The Internet Bug Bounty](#) has decided that this report is not eligible for a bounty.  
This is ineligible for award given it is low severity

May 7th (2 years ago)
-  [rafaelfranca](#) Ruby on Rails staff requested to disclose this report.

May 7th (2 years ago)
-  [rafaelfranca](#) Ruby on Rails staff disclosed this report.

May 7th (2 years ago)