



CVE-2015-7581

Published on: 02/15/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:11 PM UTC

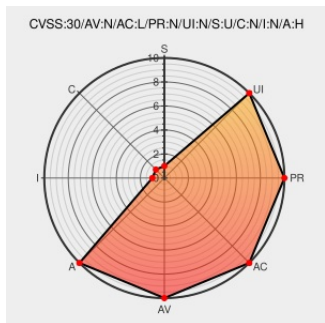
CVE-2015-7581

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [Rails](#) from [Rubyonrails](#) contain the following vulnerability:

actionpack/lib/action_dispatch/routing/route_set.rb in Action Pack in Ruby on Rails 4.x before 4.2.5.1 and 5.x before 5.0.0.beta1.1 allows remote attackers to cause a denial of service (superfluous caching and memory consumption) by leveraging an application's use of a wildcard controller route.

CVE-2015-7581 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-3464-1 rails	www.debian.org Deprecated Link text/html	DEBIAN DSA-3464

Ruby on Rails Action Pack CVE-2015-7581 Information Disclosure Vulnerability	cve.report (archive) text/html	 BID 81677
	groups.google.com text/x-ruby	 MLIST [ruby-security-ann] 20160125 [CVE-2015-7581] Object leak vulnerability for wildcard controller routes in Action Pack
Rails Multiple Bugs Let Remote Users Determine Passwords, Modify Records, Bypass Security Restrictions, Deny Service, and Conduct Cross-Site Scripting Attacks - SecurityTracker	www.securitytracker.com text/html	 SECTrack 1034816
[SECURITY] Fedora 23 Update: rubygem-actionpack-4.2.3-4.fc23	lists.fedoraproject.org text/html	 FEDORA FEDORA-2016-f486068393
[security-announce] SUSE-SU-2016:1146-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2016:1146
openSUSE-SU-2016:0372-1: moderate: Security update for rubygem-actionpac	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:0372
oss-security - [CVE-2015-7581] Object leak vulnerability for wildcard controller routes in Action Pack	www.openwall.com text/x-ruby	 MLIST [oss-security] 20160125 [CVE-2015-7581] Object leak vulnerability for wildcard controller routes in Action Pack
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2016:0296
[SECURITY] Fedora 22 Update: rubygem-activemodel-4.2.0-2.fc22	lists.fedoraproject.org text/html	 FEDORA FEDORA-2016-94e71ee673
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report .		

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rubyonrails	Rails	4.0.0	-	All	All
Application	Rubyonrails	Rails	4.0.0	beta	All	All
Application	Rubyonrails	Rails	4.0.0	rc1	All	All
Application	Rubyonrails	Rails	4.0.0	rc2	All	All
Application	Rubyonrails	Rails	4.0.1	-	All	All
Application	Rubyonrails	Rails	4.0.1	rc1	All	All
Application	Rubyonrails	Rails	4.0.1	rc2	All	All
Application	Rubyonrails	Rails	4.0.1	rc3	All	All
Application	Rubyonrails	Rails	4.0.1	rc4	All	All
Application	Rubyonrails	Rails	4.0.10	rc1	All	All

Application	Rubyonrails	Rails	4.0.2	All	All	All
Application	Rubyonrails	Rails	4.0.3	All	All	All
Application	Rubyonrails	Rails	4.0.4	All	All	All
Application	Rubyonrails	Rails	4.0.5	All	All	All
Application	Rubyonrails	Rails	4.0.6	All	All	All
Application	Rubyonrails	Rails	4.0.6	rc1	All	All
Application	Rubyonrails	Rails	4.0.6	rc2	All	All
Application	Rubyonrails	Rails	4.0.6	rc3	All	All
Application	Rubyonrails	Rails	4.0.7	All	All	All
Application	Rubyonrails	Rails	4.0.8	All	All	All
Application	Rubyonrails	Rails	4.0.9	All	All	All
Application	Rubyonrails	Rails	4.1.0	-	All	All
Application	Rubyonrails	Rails	4.1.0	beta1	All	All
Application	Rubyonrails	Rails	4.1.1	All	All	All
Application	Rubyonrails	Rails	4.1.2	All	All	All
Application	Rubyonrails	Rails	4.1.2	rc1	All	All
Application	Rubyonrails	Rails	4.1.2	rc2	All	All
Application	Rubyonrails	Rails	4.1.2	rc3	All	All
Application	Rubyonrails	Rails	4.1.3	All	All	All
Application	Rubyonrails	Rails	4.1.4	All	All	All
Application	Rubyonrails	Rails	4.1.5	All	All	All
Application	Rubyonrails	Rails	4.1.6	rc1	All	All
Application	Rubyonrails	Rails	4.1.7	All	All	All
Application	Rubyonrails	Rails	4.1.8	All	All	All
Application	Rubyonrails	Rails	4.2.0	beta1	All	All
Application	Rubyonrails	Rails	4.2.1	All	All	All
Application	Rubyonrails	Rails	4.2.2	All	All	All
Application	Rubyonrails	Rails	4.2.3	All	All	All
Application	Rubyonrails	Rails	4.2.4	All	All	All
Application	Rubyonrails	Rails	4.2.5	All	All	All
Application	Rubyonrails	Rails	5.0.0	beta1	All	All
Application	Rubyonrails	Rails	4.0.0	-	All	All
Application	Rubyonrails	Rails	4.0.0	beta	All	All
Application	Rubyonrails	Rails	4.0.0	rc1	All	All
Application	Rubyonrails	Rails	4.0.0	rc2	All	All

Application	Rubyonrails	Rails	4.0.1	-	All	All
Application	Rubyonrails	Rails	4.0.1	rc1	All	All
Application	Rubyonrails	Rails	4.0.1	rc2	All	All
Application	Rubyonrails	Rails	4.0.1	rc3	All	All
Application	Rubyonrails	Rails	4.0.1	rc4	All	All
Application	Rubyonrails	Rails	4.0.10	rc1	All	All
Application	Rubyonrails	Rails	4.0.2	All	All	All
Application	Rubyonrails	Rails	4.0.3	All	All	All
Application	Rubyonrails	Rails	4.0.4	All	All	All
Application	Rubyonrails	Rails	4.0.5	All	All	All
Application	Rubyonrails	Rails	4.0.6	All	All	All
Application	Rubyonrails	Rails	4.0.6	rc1	All	All
Application	Rubyonrails	Rails	4.0.6	rc2	All	All
Application	Rubyonrails	Rails	4.0.6	rc3	All	All
Application	Rubyonrails	Rails	4.0.7	All	All	All
Application	Rubyonrails	Rails	4.0.8	All	All	All
Application	Rubyonrails	Rails	4.0.9	All	All	All
Application	Rubyonrails	Rails	4.1.0	-	All	All
Application	Rubyonrails	Rails	4.1.0	beta1	All	All
Application	Rubyonrails	Rails	4.1.1	All	All	All
Application	Rubyonrails	Rails	4.1.2	All	All	All
Application	Rubyonrails	Rails	4.1.2	rc1	All	All
Application	Rubyonrails	Rails	4.1.2	rc2	All	All
Application	Rubyonrails	Rails	4.1.2	rc3	All	All
Application	Rubyonrails	Rails	4.1.3	All	All	All
Application	Rubyonrails	Rails	4.1.4	All	All	All
Application	Rubyonrails	Rails	4.1.5	All	All	All
Application	Rubyonrails	Rails	4.1.6	rc1	All	All
Application	Rubyonrails	Rails	4.1.7	All	All	All
Application	Rubyonrails	Rails	4.1.8	All	All	All
Application	Rubyonrails	Rails	4.2.0	beta1	All	All
Application	Rubyonrails	Rails	4.2.1	All	All	All
Application	Rubyonrails	Rails	4.2.2	All	All	All
Application	Rubyonrails	Rails	4.2.3	All	All	All
Application	Rubyonrails	Rails	4.2.4	All	All	All
Application	Rubvonrails	Rails	4.2.5	All	All	All

Application	Rubyonrails	Rails	5.0.0	beta1	All	All
cpe:2.3:a:rubyonrails:rails:4.0.0:-:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.0:beta:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.0:rc1:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.0:rc2:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.1:-:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.1:rc1:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.1:rc2:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.1:rc3:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.1:rc4:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.10:rc1:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.2:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.3:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.4:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.5:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.6:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.6:rc1:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.6:rc2:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.6:rc3:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.7:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.8:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.0.9:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.1.0:-:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.1.0:beta1:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.1.1:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.1.2:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.1.2:rc1:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:4.1.2:rc2:*:*:*:*:*:						

cpe:2.3:a:rubyonrails:rails:4.1.2:rc3:*****:
cpe:2.3:a:rubyonrails:rails:4.1.3:*****:
cpe:2.3:a:rubyonrails:rails:4.1.4:*****:
cpe:2.3:a:rubyonrails:rails:4.1.5:*****:
cpe:2.3:a:rubyonrails:rails:4.1.6:rc1:*****:
cpe:2.3:a:rubyonrails:rails:4.1.7:*****:
cpe:2.3:a:rubyonrails:rails:4.1.8:*****:
cpe:2.3:a:rubyonrails:rails:4.2.0:beta1:*****:
cpe:2.3:a:rubyonrails:rails:4.2.1:*****:
cpe:2.3:a:rubyonrails:rails:4.2.2:*****:
cpe:2.3:a:rubyonrails:rails:4.2.3:*****:
cpe:2.3:a:rubyonrails:rails:4.2.4:*****:
cpe:2.3:a:rubyonrails:rails:4.2.5:*****:
cpe:2.3:a:rubyonrails:rails:5.0.0:beta1:*****:
cpe:2.3:a:rubyonrails:rails:4.0.0:-:*****:
cpe:2.3:a:rubyonrails:rails:4.0.0:beta:*****:
cpe:2.3:a:rubyonrails:rails:4.0.0:rc1:*****:
cpe:2.3:a:rubyonrails:rails:4.0.0:rc2:*****:
cpe:2.3:a:rubyonrails:rails:4.0.1:-:*****:
cpe:2.3:a:rubyonrails:rails:4.0.1:rc1:*****:
cpe:2.3:a:rubyonrails:rails:4.0.1:rc2:*****:
cpe:2.3:a:rubyonrails:rails:4.0.1:rc3:*****:
cpe:2.3:a:rubyonrails:rails:4.0.1:rc4:*****:
cpe:2.3:a:rubyonrails:rails:4.0.10:rc1:*****:
cpe:2.3:a:rubyonrails:rails:4.0.2:*****:
cpe:2.3:a:rubyonrails:rails:4.0.3:*****:
cpe:2.3:a:rubyonrails:rails:4.0.4:*****:
cpe:2.3:a:rubyonrails:rails:4.0.5:*****:
cpe:2.3:a:rubyonrails:rails:4.0.6:*****:

```
cpe:2.3:a:rubyonrails:rails:4.0.6:rc1:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.0.6:rc2:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.0.6:rc3:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.0.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.0.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.0.9:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.1.0:-:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.1.0:beta1:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.1.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.1.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.1.2:rc1:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.1.2:rc2:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.1.2:rc3:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.1.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.1.4:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.1.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.1.6:rc1:*:*:*:*:*:
```

cpe:2.3:a:rubyonrails:rails:4.1.7:*:*:*:*:*:

```
cpe:2.3:a:rubyonrails:rails:4.1.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.2.0:beta1:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.2.1:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.2.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.2.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.2.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:4.2.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:5.0.0:beta1:.*:.*:.*:.*:.*:.*
```

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)