

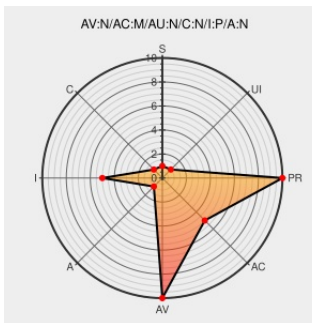


CVE-2011-2931

Published on: 08/29/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:21 PM UTC

CVE-2011-2931

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Cross-site scripting (XSS) vulnerability in the strip_tags helper in actionpack/lib/action_controller/vendor/html-scanner/html/node.rb in Ruby on Rails before 2.3.13, 3.0.x before 3.0.10, and 3.1.x before 3.1.0.rc5 allows remote attackers to inject arbitrary web script or HTML via a tag with an invalid name.

CVE-2011-2931 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

Fedora update for rubygem-actionpack - Secunia.com

[web.archive.org](#)
[text/html](#)

[SECUNIA 45921](#)

[SECURITY] Fedora 14 Update: rubygem-actionpack-2.3.8-4.fc14

[lists.fedoraproject.org](#)
[text/html](#)

[FEDORA FEDORA-2011-11567](#)

Debian -- Security Information -- DSA-2301-1 rails

[www.debian.org](#)
[Deprecated Link](#)
[text/html](#)

[DEBIAN DSA-2301](#)

oss-security - Re: CVE request: ruby on rails flaws (4)

[Patch](#)
[www.openwall.com](#)
[text/html](#)

[MLIST \[oss-security\] 20110822 Re: CVE request: ruby on rails flaws \(4\)](#)

[SECURITY] Fedora 16 Update:

[lists.fedoraproject.org](#)

[FEDORA FEDORA-2011-11386](#)

rubygem-rails-3.0.10-1.fc16	text/html	
oss-security - Re: CVE request: ruby on rails flaws (4)	www.openwall.com text/html	MLIST [oss-security] 20110822 Re: CVE request: ruby on rails flaws (4)
[SECURITY] Fedora 15 Update: rubygem-actionpack-3.0.5-4.fc15	lists.fedoraproject.org text/html	FEDORA FEDORA-2011-11572
Bug 731436 – CVE-2011-2931 rubygem-actionpack: XSS vulnerability in strip_tags helper (Ruby on Rails)	Patch bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=731436
oss-security - Re: CVE request: ruby on rails flaws (4)	Patch www.openwall.com text/html	MLIST [oss-security] 20110819 Re: CVE request: ruby on rails flaws (4)
oss-security - CVE request: ruby on rails flaws (4)	Patch www.openwall.com text/html	MLIST [oss-security] 20110817 CVE request: ruby on rails flaws (4)
Riding Rails: [ANN] Rails 3.1.0.rc6	Patch weblog.rubyonrails.org text/html	CONFIRM weblog.rubyonrails.org/2011/8/16/ann-rails-3-1-0-rc6
Google Groups	Patch groups.google.com text/html	MLIST [rubyonrails-security] 20110816 XSS Vulnerability in strip_tags helper
oss-security - Re: CVE request: ruby on rails flaws (4)	Patch www.openwall.com text/html	MLIST [oss-security] 20110822 Re: CVE request: ruby on rails flaws (4)
oss-security - Re: CVE request: ruby on rails flaws (4)	Patch www.openwall.com text/html	MLIST [oss-security] 20110820 Re: CVE request: ruby on rails flaws (4)
Tags with invalid names should also be stripped in order to prevent · rails/rails@586a944 · GitHub	Patch github.com text/html	CONFIRM github.com/rails/rails/commit/586a944ddd4d03e66dea1093306147594748037a

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	2.0.0	All	All	All
Application	Rubyonrails	Rails	2.0.0	rc1	All	All
Application	Rubyonrails	Rails	2.0.0	rc2	All	All
Application	Rubyonrails	Rails	2.0.1	All	All	All
Application	Rubyonrails	Rails	2.0.2	All	All	All
Application	Rubyonrails	Rails	2.0.4	All	All	All

Application	Rubyonrails	Rails	2.1.0	All	All	All
Application	Rubyonrails	Rails	2.1.1	All	All	All
Application	Rubyonrails	Rails	2.1.2	All	All	All
Application	Rubyonrails	Rails	2.2.0	All	All	All
Application	Rubyonrails	Rails	2.2.1	All	All	All
Application	Rubyonrails	Rails	2.2.2	All	All	All
Application	Rubyonrails	Rails	2.3.10	All	All	All
Application	Rubyonrails	Rails	2.3.11	All	All	All
Application	Rubyonrails	Rails	2.3.12	All	All	All
Application	Rubyonrails	Rails	2.3.2	All	All	All
Application	Rubyonrails	Rails	2.3.3	All	All	All
Application	Rubyonrails	Rails	2.3.4	All	All	All
Application	Rubyonrails	Rails	2.3.9	All	All	All
Application	Rubyonrails	Rails	3.0.0	All	All	All
Application	Rubyonrails	Rails	3.0.0	beta	All	All
Application	Rubyonrails	Rails	3.0.0	beta2	All	All
Application	Rubyonrails	Rails	3.0.0	beta3	All	All
Application	Rubyonrails	Rails	3.0.0	beta4	All	All
Application	Rubyonrails	Rails	3.0.0	rc	All	All
Application	Rubyonrails	Rails	3.0.0	rc2	All	All
Application	Rubyonrails	Rails	3.0.1	All	All	All
Application	Rubyonrails	Rails	3.0.1	pre	All	All
Application	Rubyonrails	Rails	3.0.10	rc1	All	All
Application	Rubyonrails	Rails	3.0.2	All	All	All
Application	Rubyonrails	Rails	3.0.2	pre	All	All
Application	Rubyonrails	Rails	3.0.3	All	All	All
Application	Rubyonrails	Rails	3.0.4	rc1	All	All
Application	Rubyonrails	Rails	3.0.5	All	All	All
Application	Rubyonrails	Rails	3.0.5	rc1	All	All
Application	Rubyonrails	Rails	3.0.6	All	All	All
Application	Rubyonrails	Rails	3.0.6	rc1	All	All
Application	Rubyonrails	Rails	3.0.6	rc2	All	All
Application	Rubyonrails	Rails	3.0.7	All	All	All
Application	Rubyonrails	Rails	3.0.7	rc1	All	All
Application	Rubyonrails	Rails	3.0.7	rc2	All	All
Application	Rubyonrails	Rails	3.0.8	All	All	All

Application	Rubyonrails	Rails	3.0.8	All	All	All
Application	Rubyonrails	Rails	3.0.8	rc1	All	All
Application	Rubyonrails	Rails	3.0.8	rc2	All	All
Application	Rubyonrails	Rails	3.0.8	rc3	All	All
Application	Rubyonrails	Rails	3.0.8	rc4	All	All
Application	Rubyonrails	Rails	3.0.9	All	All	All
Application	Rubyonrails	Rails	3.0.9	rc1	All	All
Application	Rubyonrails	Rails	3.0.9	rc2	All	All
Application	Rubyonrails	Rails	3.0.9	rc3	All	All
Application	Rubyonrails	Rails	3.0.9	rc4	All	All
Application	Rubyonrails	Rails	3.0.9	rc5	All	All
Application	Rubyonrails	Rails	3.1.0	All	All	All
Application	Rubyonrails	Rails	3.1.0	beta1	All	All
Application	Rubyonrails	Rails	3.1.0	rc1	All	All
Application	Rubyonrails	Rails	3.1.0	rc2	All	All
Application	Rubyonrails	Rails	3.1.0	rc3	All	All
Application	Rubyonrails	Rails	3.1.0	rc4	All	All
Application	Rubyonrails	Rails	2.0.0	All	All	All
Application	Rubyonrails	Rails	2.0.0	rc1	All	All
Application	Rubyonrails	Rails	2.0.0	rc2	All	All
Application	Rubyonrails	Rails	2.0.1	All	All	All
Application	Rubyonrails	Rails	2.0.2	All	All	All
Application	Rubyonrails	Rails	2.0.4	All	All	All
Application	Rubyonrails	Rails	2.1.0	All	All	All
Application	Rubyonrails	Rails	2.1.1	All	All	All
Application	Rubyonrails	Rails	2.1.2	All	All	All
Application	Rubyonrails	Rails	2.2.0	All	All	All
Application	Rubyonrails	Rails	2.2.1	All	All	All
Application	Rubyonrails	Rails	2.2.2	All	All	All
Application	Rubyonrails	Rails	2.3.10	All	All	All
Application	Rubyonrails	Rails	2.3.11	All	All	All
Application	Rubyonrails	Rails	2.3.12	All	All	All
Application	Rubyonrails	Rails	2.3.2	All	All	All
Application	Rubyonrails	Rails	2.3.3	All	All	All
Application	Rubyonrails	Rails	2.3.4	All	All	All
Application	Rubyonrails	Rails	2.3.9	All	All	All

Application	Rubyonrails	Rails	3.0.0	All	All	All
Application	Rubyonrails	Rails	3.0.0	beta	All	All
Application	Rubyonrails	Rails	3.0.0	beta2	All	All
Application	Rubyonrails	Rails	3.0.0	beta3	All	All
Application	Rubyonrails	Rails	3.0.0	beta4	All	All
Application	Rubyonrails	Rails	3.0.0	rc	All	All
Application	Rubyonrails	Rails	3.0.0	rc2	All	All
Application	Rubyonrails	Rails	3.0.1	All	All	All
Application	Rubyonrails	Rails	3.0.1	pre	All	All
Application	Rubyonrails	Rails	3.0.10	rc1	All	All
Application	Rubyonrails	Rails	3.0.2	All	All	All
Application	Rubyonrails	Rails	3.0.2	pre	All	All
Application	Rubyonrails	Rails	3.0.3	All	All	All
Application	Rubyonrails	Rails	3.0.4	rc1	All	All
Application	Rubyonrails	Rails	3.0.5	All	All	All
Application	Rubyonrails	Rails	3.0.5	rc1	All	All
Application	Rubyonrails	Rails	3.0.6	All	All	All
Application	Rubyonrails	Rails	3.0.6	rc1	All	All
Application	Rubyonrails	Rails	3.0.6	rc2	All	All
Application	Rubyonrails	Rails	3.0.7	All	All	All
Application	Rubyonrails	Rails	3.0.7	rc1	All	All
Application	Rubyonrails	Rails	3.0.7	rc2	All	All
Application	Rubyonrails	Rails	3.0.8	All	All	All
Application	Rubyonrails	Rails	3.0.8	rc1	All	All
Application	Rubyonrails	Rails	3.0.8	rc2	All	All
Application	Rubyonrails	Rails	3.0.8	rc3	All	All
Application	Rubyonrails	Rails	3.0.8	rc4	All	All
Application	Rubyonrails	Rails	3.0.9	All	All	All
Application	Rubyonrails	Rails	3.0.9	rc1	All	All
Application	Rubyonrails	Rails	3.0.9	rc2	All	All
Application	Rubyonrails	Rails	3.0.9	rc3	All	All
Application	Rubyonrails	Rails	3.0.9	rc4	All	All
Application	Rubyonrails	Rails	3.0.9	rc5	All	All
Application	Rubyonrails	Rails	3.1.0	All	All	All
Application	Rubyonrails	Rails	3.1.0	beta1	All	All

Application	Rubyonrails	Rails	3.1.0	rc1	All	All
Application	Rubyonrails	Rails	3.1.0	rc2	All	All
Application	Rubyonrails	Rails	3.1.0	rc3	All	All
Application	Rubyonrails	Rails	3.1.0	rc4	All	All
Application	Rubyonrails	Ruby On Rails	3.0.4	All	All	All
Application	Rubyonrails	Ruby On Rails	3.0.4	All	All	All
cpe:2.3:a:rubyonrails:rails:2.0.0:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:2.0.0:rc1:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:2.0.0:rc2:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:2.0.1:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:2.0.2:*:*:*:*::~						
cpe:2.3:a:rubyonrails:rails:2.0.4:*:*:*:*::~						
cpe:2.3:a:rubyonrails:rails:2.1.0:*:*:*:*::~						
cpe:2.3:a:rubyonrails:rails:2.1.1:*:*:*:*::~						
cpe:2.3:a:rubyonrails:rails:2.1.2:*:*:*:*::~						
cpe:2.3:a:rubyonrails:rails:2.2.0:*:*:*:*::~						
cpe:2.3:a:rubyonrails:rails:2.2.1:*:*:*:*::~						
cpe:2.3:a:rubyonrails:rails:2.2.2:*:*:*:*::~						
cpe:2.3:a:rubyonrails:rails:2.3.10:*:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:2.3.11:*:*:*:*::~						
cpe:2.3:a:rubyonrails:rails:2.3.12:*:*:*:*::~						
cpe:2.3:a:rubyonrails:rails:2.3.2:*:*:*:*::~						
cpe:2.3:a:rubyonrails:rails:2.3.3:*:*:*:*::~						
cpe:2.3:a:rubyonrails:rails:2.3.4:*:*:*:*::~						
cpe:2.3:a:rubyonrails:rails:2.3.9:*:*:*:*::~						
cpe:2.3:a:rubyonrails:rails:3.0.0:*:*:*:*::~						
cpe:2.3:a:rubyonrails:rails:3.0.0:beta:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:3.0.0:beta2:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:3.0.0:beta3:*:*:*:*:						
cpe:2.3:a:rubyonrails:rails:3.0.0:beta4:*:*:*:*:						

cpe:2.3:a:rubyonrails:rails:3.0.0:rc:****:
cpe:2.3:a:rubyonrails:rails:3.0.0:rc2:****:
cpe:2.3:a:rubyonrails:rails:3.0.1:****:
cpe:2.3:a:rubyonrails:rails:3.0.1:pre:****:
cpe:2.3:a:rubyonrails:rails:3.0.10:rc1:****:
cpe:2.3:a:rubyonrails:rails:3.0.2:****:
cpe:2.3:a:rubyonrails:rails:3.0.2:pre:****:
cpe:2.3:a:rubyonrails:rails:3.0.3:****:
cpe:2.3:a:rubyonrails:rails:3.0.4:rc1:****:
cpe:2.3:a:rubyonrails:rails:3.0.5:****:
cpe:2.3:a:rubyonrails:rails:3.0.5:rc1:****:
cpe:2.3:a:rubyonrails:rails:3.0.6:****:
cpe:2.3:a:rubyonrails:rails:3.0.6:rc1:****:
cpe:2.3:a:rubyonrails:rails:3.0.6:rc2:****:
cpe:2.3:a:rubyonrails:rails:3.0.7:****:
cpe:2.3:a:rubyonrails:rails:3.0.7:rc1:****:
cpe:2.3:a:rubyonrails:rails:3.0.7:rc2:****:
cpe:2.3:a:rubyonrails:rails:3.0.8:****:
cpe:2.3:a:rubyonrails:rails:3.0.8:rc1:****:
cpe:2.3:a:rubyonrails:rails:3.0.8:rc2:****:
cpe:2.3:a:rubyonrails:rails:3.0.8:rc3:****:
cpe:2.3:a:rubyonrails:rails:3.0.8:rc4:****:
cpe:2.3:a:rubyonrails:rails:3.0.9:****:
cpe:2.3:a:rubyonrails:rails:3.0.9:rc1:****:
cpe:2.3:a:rubyonrails:rails:3.0.9:rc2:****:
cpe:2.3:a:rubyonrails:rails:3.0.9:rc3:****:
cpe:2.3:a:rubyonrails:rails:3.0.9:rc4:****:
cpe:2.3:a:rubyonrails:rails:3.0.9:rc5:****:

```
cpe:2.3:a:rubyonrails:rails:3.1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.1.0:beta1:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.1.0:rc1:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.1.0:rc2:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.1.0:rc3:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.1.0:rc4:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:2.0.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:2.0.0:rc1:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:2.0.0:rc2:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:2.0.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:2.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:2.0.4:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:2.1.0:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:2.1.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:2.1.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:2.2.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:2.2.1:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:2.2.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:2.3.10:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:2.3.11:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:2.3.12:*:*:*:*:*:*
```

```
cpe:2.3:a:rubyonrails:rails:2.3.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:2.3.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:2.3.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:2.3.9:*:*:*:*:*:*
```

```
cpe:2.3:a:rubyonrails:rails:3.0.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.0:beta:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.0:beta2:*:*:*:*:*:
```

```
cne:2.3:a:rubyonrails:rails:3.0.0:beta3:***.***.
```

cpe:2.3:a:rubyonrails:rails:3.0.0:beta4:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.0:rc:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.0:rc2:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.1:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.1:pre:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.10:rc1:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.2:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.2:pre:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.3:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.4:rc1:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.5:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.5:rc1:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.6:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.6:rc1:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.6:rc2:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.7:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.7:rc1:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.7:rc2:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.8:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.8:rc1:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.8:rc2:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.8:rc3:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.8:rc4:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.9:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.9:rc1:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.9:rc2:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.9:rc3:****:*:
cpe:2.3:a:rubyonrails:rails:3.0.9:rc4:****:*:

cpe:2.3:a:rubyonrails:rails:3.0.9:rc5:*****:
cpe:2.3:a:rubyonrails:rails:3.1.0:*****:
cpe:2.3:a:rubyonrails:rails:3.1.0:beta1:*****:
cpe:2.3:a:rubyonrails:rails:3.1.0:rc1:*****:
cpe:2.3:a:rubyonrails:rails:3.1.0:rc2:*****:
cpe:2.3:a:rubyonrails:rails:3.1.0:rc3:*****:
cpe:2.3:a:rubyonrails:rails:3.1.0:rc4:*****:
cpe:2.3:a:rubyonrails:ruby_on_rails:3.0.4:*****:
cpe:2.3:a:rubyonrails:ruby_on_rails:3.0.4:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [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](#)