



CVE-2011-2197

Published on: 06/30/2011 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:22 AM UTC

CVE-2011-2197

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

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

The cross-site scripting (XSS) prevention feature in Ruby on Rails 2.x before 2.3.12, 3.0.x before 3.0.8, and 3.1.x before 3.1.0.rc2 does not properly handle mutation of safe buffers, which makes it easier for remote attackers to conduct XSS attacks via crafted strings to an application that uses a problematic string method, as demonstrated by

the sub method.

CVE-2011-2197 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

PARTIAL

NONE

CVE References

Description

Tags

Link

Google Groups

[Patch](#)
[groups.google.com](#)
[text/html](#)

[MLIST \[rubyonrails-security\] 20110607 Potential XSS Vulnerability in Ruby on Rails Applications](#)

[SECURITY] Fedora 15 Update: rubygem-actionpack-3.0.5-3.fc15

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

[FEDORA FEDORA-2011-8580](#)

oss-security - CVE Request: Ruby on Rails 3/rails_xss XSS

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

[MLIST \[oss-security\] 20110609 CVE Request: Ruby on Rails 3/rails_xss XSS](#)

Riding Rails: Potential XSS Vulnerability in Ruby on Rails Applications

[Patch](#)
[weblog.rubyonrails.org](#)
[text/html](#)

[CONFIRM weblog.rubyonrails.org/2011/6/8/potential-xss-vulnerability-in-ruby-on-rails-applications](#)

oss-security - Re: CVE Request: Ruby on Rails 3/rails_xss XSS	Patch openwall.com text/html	 MLIST [oss-security] 20110613 Re: CVE Request: Ruby on Rails 3/rails_xss XSS
Ruby on Rails Safe Buffer Cross-Site Scripting Weakness - Secunia.com	Vendor Advisory web.archive.org text/html	 SECUNIA 44789
[SECURITY] Fedora 15 Update: rubygem-activesupport-3.0.5-3.fc15	lists.fedoraproject.org text/html	 FEDORA FEDORA-2011-8494

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	2.3.2	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	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	3.0.2	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	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	3.1.0	All	All	All
Application	Rubyonrails	Rails	3.1.0	beta1	All	All
Application	Rubyonrails	Rails	3.1.0	rc1	All	All
Application	Rubyonrails	Rails	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	2.3.2	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	3.0.2	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	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	3.1.0	All	All	All
Application	Rubyonrails	Rails	3.1.0	beta1	All	All
Application	Rubyonrails	Rails	3.1.0	rc1	All	All

Application	Rubyonrails	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:2.3.2:*:*:*:*:*:						
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:3.0.2:*****:
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: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:3.1.0:*****:
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: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:2.3.2:*****:
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:3.0.2:*****:
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: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:3.1.0:~::~~::~~::~~::~~::~~:::
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: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 →](#)