



CVE-2014-0130

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2014-0130
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-07 10:55:00 UTC
Updated	2023-02-13 00:32:00 UTC
Description	Directory traversal vulnerability in actionpack/lib/abstract_controller/base.rb in the implicit-render implementation in Ruby or

Risk And Classification

EPSS: 0.453740000 probability, percentile 0.975830000 (date 2026-04-01)

CISA KEV: Listed on 2022-03-25; due 2022-04-15; ransomware use Unknown

Problem Types: CWE-22

CISA Known Exploited Vulnerability

Vendor	Rails
Product	Ruby on Rails
Name	Ruby on Rails Directory Traversal Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2014-0130

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Subscription Asset Manager	All	All	All	All
Application	Rubyonrails	Rails	4.1.0	-	All	All
Application	Rubyonrails	Rails	4.1.0	-	All	All
Application	Rubyonrails	Rails	3.2.0	All	All	All
Application	Rubyonrails	Rails	3.2.0	rc1	All	All
Application	Rubyonrails	Rails	3.2.0	rc2	All	All
Application	Rubyonrails	Rails	3.2.1	All	All	All
Application	Rubyonrails	Rails	3.2.10	All	All	All

Application	Rubyonrails	Rails	3.2.11	All	All	All
Application	Rubyonrails	Rails	3.2.12	All	All	All
Application	Rubyonrails	Rails	3.2.13	rc1	All	All
Application	Rubyonrails	Rails	3.2.13	rc2	All	All
Application	Rubyonrails	Rails	3.2.15	rc3	All	All
Application	Rubyonrails	Rails	3.2.16	All	All	All
Application	Rubyonrails	Rails	3.2.2	All	All	All
Application	Rubyonrails	Rails	3.2.2	rc1	All	All
Application	Rubyonrails	Rails	3.2.3	All	All	All
Application	Rubyonrails	Rails	3.2.3	rc1	All	All
Application	Rubyonrails	Rails	3.2.3	rc2	All	All
Application	Rubyonrails	Rails	3.2.4	All	All	All
Application	Rubyonrails	Rails	3.2.4	rc1	All	All
Application	Rubyonrails	Rails	3.2.5	All	All	All
Application	Rubyonrails	Rails	3.2.6	All	All	All
Application	Rubyonrails	Rails	3.2.7	All	All	All
Application	Rubyonrails	Rails	3.2.8	All	All	All
Application	Rubyonrails	Rails	3.2.9	All	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	4.0.2	All	All	All
Application	Rubyonrails	Rails	4.0.3	All	All	All
Application	Rubyonrails	Rails	4.0.4	All	All	All
Application	Rubyonrails	Rails	4.1.0	beta1	All	All
Application	Rubyonrails	Rails	3.2.0	All	All	All
Application	Rubyonrails	Rails	3.2.0	rc1	All	All
Application	Rubyonrails	Rails	3.2.0	rc2	All	All
Application	Rubyonrails	Rails	3.2.1	All	All	All

Application	Rubyonrails	Rails	3.2.10	All	All	All
Application	Rubyonrails	Rails	3.2.11	All	All	All
Application	Rubyonrails	Rails	3.2.12	All	All	All
Application	Rubyonrails	Rails	3.2.13	rc1	All	All
Application	Rubyonrails	Rails	3.2.13	rc2	All	All
Application	Rubyonrails	Rails	3.2.15	rc3	All	All
Application	Rubyonrails	Rails	3.2.16	All	All	All
Application	Rubyonrails	Rails	3.2.2	All	All	All
Application	Rubyonrails	Rails	3.2.2	rc1	All	All
Application	Rubyonrails	Rails	3.2.3	All	All	All
Application	Rubyonrails	Rails	3.2.3	rc1	All	All
Application	Rubyonrails	Rails	3.2.3	rc2	All	All
Application	Rubyonrails	Rails	3.2.4	All	All	All
Application	Rubyonrails	Rails	3.2.4	rc1	All	All
Application	Rubyonrails	Rails	3.2.5	All	All	All
Application	Rubyonrails	Rails	3.2.6	All	All	All
Application	Rubyonrails	Rails	3.2.7	All	All	All
Application	Rubyonrails	Rails	3.2.8	All	All	All
Application	Rubyonrails	Rails	3.2.9	All	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	4.0.2	All	All	All
Application	Rubyonrails	Rails	4.0.3	All	All	All
Application	Rubyonrails	Rails	4.0.4	All	All	All
Application	Rubyonrails	Rails	4.1.0	beta1	All	All
Application	Rubyonrails	Ruby On Rails	All	All	All	All

References

Reference

Source

Link

[rubyonrails-security] 20140506 [CVE-2014-0130] Directory Traversal Vulnerability With Certain Route Configurations	MLIST	groups.g
access.redhat.com CVE-2014-0130	MISC	access.r
Red Hat Customer Portal	MISC	access.r
Red Hat Customer Portal	MISC	access.r
matasano.com/research/AnatomyOfRailsVuln-CVE-2014-0130.pdf	MISC	matasan
Ruby on Rails 'implicit render' Functionality Directory Traversal Vulnerability	BID	www.sec
1095105 – (CVE-2014-0130) CVE-2014-0130 rubygem-actionpack: directory traversal issue	MISC	bugzilla.r
Red Hat Customer Portal	REDHAT	rhn.redh
Red Hat Customer Portal	MISC	access.r
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#)