



CVE-2015-7576

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2015-7576
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-02-16 02:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The http_basic_authenticate_with method in actionpack/lib/action_controller/metal/http_authentication.rb in the Basic Authen

Risk And Classification

Primary CVSS: v3.0 3.7 LOW from nvd@nist.gov

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

Problem Types: CWE-254 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	3.7	LOW	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
2.0	nvd@nist.gov	Primary	4.3		AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:M/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

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	All	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	4.0.4	rc1	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	4.1.0	beta2	All	All
Application	Rubyonrails	Rails	4.1.0	rc1	All	All
Application	Rubyonrails	Rails	4.1.0	rc2	All	All
Application	Rubyonrails	Rails	4.1.1	All	All	All
Application	Rubyonrails	Rails	4.1.10	All	All	All
Application	Rubyonrails	Rails	4.1.10	rc1	All	All
Application	Rubyonrails	Rails	4.1.10	rc2	All	All
Application	Rubyonrails	Rails	4.1.10	rc3	All	All
Application	Rubyonrails	Rails	4.1.10	rc4	All	All
Application	Rubyonrails	Rails	4.1.12	All	All	All
Application	Rubyonrails	Rails	4.1.12	rc1	All	All
Application	Rubyonrails	Rails	4.1.13	All	All	All
Application	Rubyonrails	Rails	4.1.13	rc1	All	All
Application	Rubyonrails	Rails	4.1.14	All	All	All
Application	Rubyonrails	Rails	4.1.14	rc1	All	All
Application	Rubyonrails	Rails	4.1.14	rc2	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	All	All	All
Application	Rubyonrails	Rails	4.1.6	rc1	All	All
Application	Rubyonrails	Rails	4.1.6	rc2	All	All
Application	Rubyonrails	Rails	4.1.7	All	All	All
Application	Rubyonrails	Rails	4.1.7	All	All	All

Application	Rubyonrails	Rails	4.1./1	All	All	All
Application	Rubyonrails	Rails	4.1.8	All	All	All
Application	Rubyonrails	Rails	4.1.9	All	All	All
Application	Rubyonrails	Rails	4.1.9	rc1	All	All
Application	Rubyonrails	Rails	4.2.0	All	All	All
Application	Rubyonrails	Rails	4.2.0	beta1	All	All
Application	Rubyonrails	Rails	4.2.0	beta2	All	All
Application	Rubyonrails	Rails	4.2.0	beta3	All	All
Application	Rubyonrails	Rails	4.2.0	beta4	All	All
Application	Rubyonrails	Rails	4.2.0	rc1	All	All
Application	Rubyonrails	Rails	4.2.0	rc2	All	All
Application	Rubyonrails	Rails	4.2.0	rc3	All	All
Application	Rubyonrails	Rails	4.2.1	All	All	All
Application	Rubyonrails	Rails	4.2.1	rc1	All	All
Application	Rubyonrails	Rails	4.2.1	rc2	All	All
Application	Rubyonrails	Rails	4.2.1	rc3	All	All
Application	Rubyonrails	Rails	4.2.1	rc4	All	All
Application	Rubyonrails	Rails	4.2.2	All	All	All
Application	Rubyonrails	Rails	4.2.3	All	All	All
Application	Rubyonrails	Rails	4.2.3	rc1	All	All
Application	Rubyonrails	Rails	4.2.4	All	All	All
Application	Rubyonrails	Rails	4.2.4	rc1	All	All
Application	Rubyonrails	Rails	4.2.5	All	All	All
Application	Rubyonrails	Rails	4.2.5	rc1	All	All
Application	Rubyonrails	Rails	4.2.5	rc2	All	All
Application	Rubyonrails	Rails	5.0.0	beta1	All	All
Application	Rubyonrails	Ruby On Rails	4.0.10	rc2	All	All
Application	Rubyonrails	Ruby On Rails	4.0.11	All	All	All
Application	Rubyonrails	Ruby On Rails	4.0.11.1	All	All	All
Application	Rubyonrails	Ruby On Rails	4.0.12	All	All	All
Application	Rubyonrails	Ruby On Rails	4.0.13	All	All	All
Application	Rubyonrails	Ruby On Rails	4.0.13	rc1	All	All
Application	Rubyonrails	Ruby On Rails	4.1.11	All	All	All
Application	Rubyonrails	Ruby On Rails	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference

Rails Multiple Bugs Let Remote Users Determine Passwords, Modify Records, Bypass Security Restrictions, Deny Service, and Conduct Cross

openSUSE-SU-2016:0372-1: moderate: Security update for rubygem-actionpac

[SECURITY] Fedora 23 Update: rubygem-actionpack-4.2.3-4.fc23

[SECURITY] Fedora 22 Update: rubygem-activemodel-4.2.0-2.fc22

Debian -- Security Information -- DSA-3464-1 rails

Ruby On Rails Action Controller CVE-2015-7576 Information Disclosure Vulnerability

[security-announce] SUSE-SU-2016:1146-1: important: Security update for

Red Hat Customer Portal

groups.google.com/forum/message/raw

oss-security - [CVE-2015-7576] Timing attack vulnerability in basic authentication in Action Controller.

openSUSE-SU-2016:0363-1: moderate: Security update for rubygem-actionpac

[SECURITY] Fedora 22 Update: rubygem-activesupport-4.2.0-4.fc22

[SECURITY] Fedora 23 Update: rubygem-activesupport-4.2.3-3.fc23

CVE Program record

NVD vulnerability detail

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](#).

Free **CVE JSON API** [cve.report/api](#)

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