



CVE-2009-3009

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2009-3009
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-09-08 18:30:00 UTC
Updated	2019-08-08 14:43:00 UTC
Description	Cross-site scripting (XSS) vulnerability in Ruby on Rails 2.x before 2.2.3, and 2.3.x before 2.3.4, allows remote attackers to

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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	2.3.2	All	All	All
Application	Rubyonrails	Rails	2.3.3	All	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	2.3.2	All	All	All
Application	Rubyonrails	Rails	2.3.3	All	All	All

References	
Reference	Source
IBM X-Force Exchange	XF
Ruby on Rails Form Helpers Unicode String Handling Cross Site Scripting Vulnerability	BID
Ruby on Rails Unicode Input Cross-Site Scripting Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
XSS Vulnerability in Ruby on Rails - Ruby on Rails: Security Google Groups	MLIST
#545063 - Security fixes (incl. CVE-2009-3009) - Debian Bug report logs	CONFIRM
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
APPLE-SA-2010-03-29-1 Security Update 2010-002 / Mac OS X v10.6.3	APPLE
Ruby on Rails Input Validation Flaw in Form Helpers Permits Cross-Site Scripting Attacks - SecurityTracker	SECTrack
Debian update for rails - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
57666	OSVDB
Debian -- Security Information -- DSA-1887-1 rails	DEBIAN
Riding Rails: XSS Vulnerability in Ruby on Rails	CONFIRM
About the security content of Security Update 2010-002 / Mac OS X v10.6.3	CONFIRM
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:017	SUSE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)