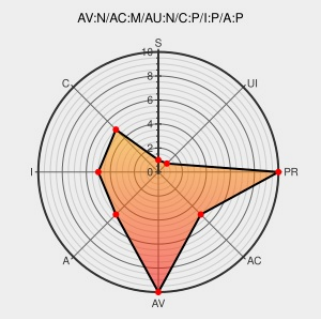
CVE-2008-7248

Published on: 12/15/2009 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:19:00 AM UTC

CVE-2008-7248

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Rails from Rubyonrails contain the following vulnerability:

Ruby on Rails 2.1 before 2.1.3 and 2.2.x before 2.2.2 does not verify tokens for requests with certain content types, which allows remote attackers to bypass cross-site request forgery (CSRF) protection for requests to applications that rely on this protection, as demonstrated using text/plain.

CVE-2008-7248 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
CVE-2008-7248 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2008-7248
oss-security - Re: CVE request: Ruby on Rails: CSRF circumvention (from 2008)	www.openwall.com text/html	MLIST [oss-security] 20091202 Re: CVE request: Ruby on Rails: CSRF circumvention (from 2008)
Riding Rails: Potential Circumvention of CSRF Protection in Rails 2.1	weblog.rubyonrails.org text/html	CONFIRM weblog.rubyonrails.org/2008/11/18/potential-circumvention-of-csrf-protection-in-rails-2-1
Ruby on Rails Unicode Input Cross-Site Scripting Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 36600

[security-announce] SUSE Security Summary Report: SUSE-SR:2010:006	lists.opensuse.org text/html	SUSE SUSE-SR:2010:006
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2009-2544
Ruby on Rails Security Project - Journal - Circumvent Rails CSRF Protection	Exploit www.rorsecurity.info text/html	MISC www.rorsecurity.info/journal/2008/11/19/circumvent-rails-csrf-protection.html
SUSE Update for Multiple Packages - Advisories - Community	web.archive.org text/html	SECUNIA 38915
Form Data Encoding Roundup	pseudo-flaw.net text/xml	MISC pseudo-flaw.net/content/web-browsers/form-data-encoding-roundup/
oss-security - CVE request: Ruby on Rails: CSRF circumvention (from 2008)	www.openwall.com text/html	MLIST [oss-security] 20091128 CVE request: Ruby on Rails: CSRF circumvention (from 2008)
544329 – (CVE-2008-7248) CVE-2008-7248 rubygem-actionpack: Potential CSRF protection circumvention	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=544329
Potential Circumvention of CSRF Protection in Rails 2.1 - Ruby on Rails: Security | Google Groups	groups.google.com text/html	MISC groups.google.com/group/rubyonrails-security/browse_thread/thread/d741ee286e36e301?hl=en

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	2.1.0	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	2.1.0	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

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:2.1.0:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→