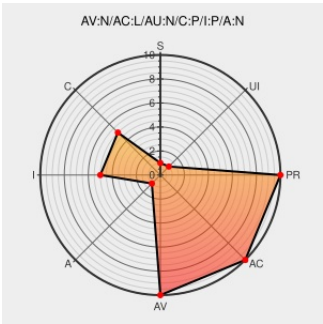
CVE-2013-0155

Published on: 01/13/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:40 PM UTC

CVE-2013-0155

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

Ruby on Rails 3.0.x before 3.0.19, 3.1.x before 3.1.10, and 3.2.x before 3.2.11 does not properly consider differences in parameter handling between the Active Record component and the JSON implementation, which allows remote attackers to bypass intended database-query restrictions and perform NULL checks or trigger missing WHERE clauses via a crafted request, as demonstrated by certain "[nil]" values, a related issue to CVE-2012-2660 and CVE-2012-2694.

CVE-2013-0155 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
openSUSE-SU-2013:1907-1: moderate: update for rubygem-actionpack-3_2	Mailing List, Third Party Advisory, lists.opensuse.org, text/html	SUSE openSUSE-SU-2013:1907
CVE-2013-0155 | Puppet	Third Party Advisory, puppet.com, text/html	CONFIRM puppet.com/security/cve/cve-2013-0155
Red Hat Customer Portal	Third Party Advisory, web.archive.org, text/html	REDHAT RHSA-2013:0154

	Inactive Link Not Archived	
Debian -- Security Information -- DSA-2609-1 rails	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-2609
openSUSE-SU-2013:1906-1: moderate: update for rubygem-actionpack-3_2	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1906
Wonderware Intelligence Tableau Server Ruby on Rails Improper Input Validation (Update A) | ICS-CERT	Third Party Advisory US Government Resource web.archive.org text/html Inactive Link Not Archived	MISC ics-cert.us-cert.gov/advisories/ICSA-13-036-01A
Google Groups	Third Party Advisory groups.google.com text/html	MLIST [rubyonrails-security] 20130108 Unsafe Query Generation Risk in Ruby on Rails (CVE-2013-0155)
openSUSE-SU-2013:1904-1: moderate: update for rubygem-actionpack-3_2	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1904
APPLE-SA-2013-06-04-1 OS X Mountain Lion v10.8.4 and Security Update 2013-002	Mailing List Third Party Advisory lists.apple.com text/html	APPLE APPLE-SA-2013-06-04-1
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0155
openSUSE-SU-2014:0009-1: moderate: update for rubygem-actionpack-3_2	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2014:0009
About the security content of OS X Mountain Lion v10.8.4 and Security Update 2013-002	Third Party Advisory support.apple.com text/html	CONFIRM support.apple.com/kb/HT5784

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Application	Rubyonrails	Rails	All	All	All	All

Application	Rubyonrails	Rails	All	All	All	All
Application	Rubyonrails	Ruby On Rails	All	All	All	All
Application	Rubyonrails	Ruby On Rails	All	All	All	All

cpe:2.3:o:debian:debian_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:*:*:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:*:*:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:ruby_on_rails:*:*:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:ruby_on_rails:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→