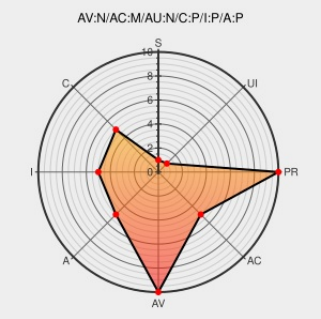
# CVE-2014-0080

Published on: 02/20/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:56 PM UTC

## CVE-2014-0080

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




Certain versions of Rails from Rubyonrails contain the following vulnerability:

SQL injection vulnerability in activerecord/lib/active_record/connection_adapters/postgresql/cast.rb in Active Record in Ruby on Rails 4.0.x before 4.0.3, and 4.1.0.beta1, when PostgreSQL is used, allows remote attackers to execute "add data" SQL commands via vectors involving \ (backslash) characters that are not properly handled in operations on array columns.

CVE-2014-0080 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 |
|---|---|---|
| | groups.google.com<br>text/plain | MLIST [rubyonrails-security] 20140218 Data Injection Vulnerability in Active Record (CVE-2014-0080) |
| oss-security - Data Injection Vulnerability in Active Record (CVE-2014-0080) | openwall.com<br>text/x-ruby | MLIST [oss-security] 20140218 Data Injection Vulnerability in Active Record (CVE-2014-0080) |

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 | 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 | 4.1.0 | beta1 | 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 | 4.1.0 | beta1 | All | All |

cpe:2.3:a:rubyonrails:rails:4.0.0:-:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.0.0:beta:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.0.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.0.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.0.1:-:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.0.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.0.1:rc2:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.0.1:rc3:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.0.1:rc4:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.1.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.0.0:-:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.0.0:beta:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.0.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.0.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.0.1:-:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.0.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.0.1:rc2:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.0.1:rc3:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.0.1:rc4:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:rubyonrails:rails:4.1.0:beta1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→