

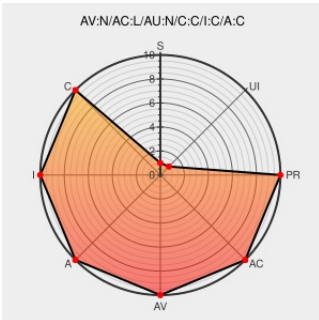


CVE-2013-0277

Published on: 02/12/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:25 AM UTC

CVE-2013-0277

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Rails](#) from [Rubyonrails](#) contain the following vulnerability:

ActiveRecord in Ruby on Rails before 2.3.17 and 3.x before 3.1.0 allows remote attackers to cause a denial of service or execute arbitrary code via crafted serialized attributes that cause the +serialize+ helper to deserialize arbitrary YAML.

CVE-2013-0277 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

No Description Provided

www.osvdb.org

OSVDB 90073

Inactive Link Not Archived

Google Groups

groups.google.com
text/html

MLIST [rubyonrails-security] 20130211 Serialized Attributes YAML Vulnerability with Rails 2.3 and 3.0 [CVE-2013-0277]

Security Advisory SA52112 - Ruby on Rails Two Vulnerabilities - Secunia

web.archive.org
text/html

SECUNIA 52112

CVE-2013-0277 | Puppet

puppet.com
text/html

CONFIRM puppet.com/security/cve/cve-2013-0277

oss-security - Serialized Attributes YAML Vulnerability with Rails 2.3 and 3.0 [CVE-2013-0277]

Patch
www.openwall.com
text/x-ruby

MLIST [oss-security] 20130211 Serialized Attributes YAML Vulnerability with Rails 2.3 and 3.0 [CVE-2013-0277]

openSUSE-SU-2013:0462-1: moderate: RubyOnRails: security version update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:0462
Rails Serialized Attributes Processing Flaw Lets Remote Users Execute Arbitrary Code and Deny Service - SecurityTracker	securitytracker.com text/html	 SECTRACK 1028109
APPLE-SA-2013-06-04-1 OS X Mountain Lion v10.8.4 and Security Update 2013-002	lists.apple.com text/html	 APPLE APPLE-SA-2013-06-04-1
Riding Rails: [SEC][ANN] Rails 3.2.12, 3.1.11, and 2.3.17 have been released!	weblog.rubyonrails.org text/html	 CONFIRM weblog.rubyonrails.org/2013/2/11/SEC-ANN-Rails-3-2-12-3-1-11-and-2-3-17-have-been-released/
About the security content of OS X Mountain Lion v10.8.4 and Security Update 2013-002	support.apple.com text/html	 CONFIRM support.apple.com/kb/HT5784
Debian -- Security Information -- DSA-2620-1 rails	www.debian.org Deprecated Link text/html	 DEBIAN DSA-2620

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	2.3.0	All	All	All
Application	Rubyonrails	Rails	2.3.1	All	All	All
Application	Rubyonrails	Rails	2.3.10	All	All	All
Application	Rubyonrails	Rails	2.3.11	All	All	All
Application	Rubyonrails	Rails	2.3.12	All	All	All
Application	Rubyonrails	Rails	2.3.13	All	All	All
Application	Rubyonrails	Rails	2.3.14	All	All	All
Application	Rubyonrails	Rails	2.3.15	All	All	All
Application	Rubyonrails	Rails	2.3.16	All	All	All
Application	Rubyonrails	Rails	2.3.2	All	All	All
Application	Rubyonrails	Rails	2.3.3	All	All	All
Application	Rubyonrails	Rails	2.3.4	All	All	All
Application	Rubyonrails	Rails	2.3.9	All	All	All
Application	Rubyonrails	Rails	3.0.0	All	All	All
Application	Rubyonrails	Rails	3.0.0	beta	All	All
Application	Rubyonrails	Rails	3.0.0	beta2	All	All

Application	Rubyonrails	Rails	3.0.0	beta3	All	All
Application	Rubyonrails	Rails	3.0.0	beta4	All	All
Application	Rubyonrails	Rails	3.0.0	rc	All	All
Application	Rubyonrails	Rails	3.0.0	rc2	All	All
Application	Rubyonrails	Rails	3.0.1	All	All	All
Application	Rubyonrails	Rails	3.0.1	pre	All	All
Application	Rubyonrails	Rails	3.0.10	All	All	All
Application	Rubyonrails	Rails	3.0.10	rc1	All	All
Application	Rubyonrails	Rails	3.0.11	All	All	All
Application	Rubyonrails	Rails	3.0.12	All	All	All
Application	Rubyonrails	Rails	3.0.12	rc1	All	All
Application	Rubyonrails	Rails	3.0.13	All	All	All
Application	Rubyonrails	Rails	3.0.13	rc1	All	All
Application	Rubyonrails	Rails	3.0.14	All	All	All
Application	Rubyonrails	Rails	3.0.16	All	All	All
Application	Rubyonrails	Rails	3.0.17	All	All	All
Application	Rubyonrails	Rails	3.0.18	All	All	All
Application	Rubyonrails	Rails	3.0.19	All	All	All
Application	Rubyonrails	Rails	3.0.2	All	All	All
Application	Rubyonrails	Rails	3.0.2	pre	All	All
Application	Rubyonrails	Rails	3.0.20	All	All	All
Application	Rubyonrails	Rails	3.0.3	All	All	All
Application	Rubyonrails	Rails	3.0.4	rc1	All	All
Application	Rubyonrails	Rails	3.0.5	All	All	All
Application	Rubyonrails	Rails	3.0.5	rc1	All	All
Application	Rubyonrails	Rails	3.0.6	All	All	All
Application	Rubyonrails	Rails	3.0.6	rc1	All	All
Application	Rubyonrails	Rails	3.0.6	rc2	All	All
Application	Rubyonrails	Rails	3.0.7	All	All	All
Application	Rubyonrails	Rails	3.0.7	rc1	All	All
Application	Rubyonrails	Rails	3.0.7	rc2	All	All
Application	Rubyonrails	Rails	3.0.8	All	All	All
Application	Rubyonrails	Rails	3.0.8	rc1	All	All
Application	Rubyonrails	Rails	3.0.8	rc2	All	All
Application	Rubyonrails	Rails	3.0.8	rc3	All	All

Application	Rubyonrails	Rails	3.0.8	rc4	All	All
Application	Rubyonrails	Rails	3.0.9	All	All	All
Application	Rubyonrails	Rails	3.0.9	rc1	All	All
Application	Rubyonrails	Rails	3.0.9	rc2	All	All
Application	Rubyonrails	Rails	3.0.9	rc3	All	All
Application	Rubyonrails	Rails	3.0.9	rc4	All	All
Application	Rubyonrails	Rails	3.0.9	rc5	All	All
Application	Rubyonrails	Rails	2.3.0	All	All	All
Application	Rubyonrails	Rails	2.3.1	All	All	All
Application	Rubyonrails	Rails	2.3.10	All	All	All
Application	Rubyonrails	Rails	2.3.11	All	All	All
Application	Rubyonrails	Rails	2.3.12	All	All	All
Application	Rubyonrails	Rails	2.3.13	All	All	All
Application	Rubyonrails	Rails	2.3.14	All	All	All
Application	Rubyonrails	Rails	2.3.15	All	All	All
Application	Rubyonrails	Rails	2.3.16	All	All	All
Application	Rubyonrails	Rails	2.3.2	All	All	All
Application	Rubyonrails	Rails	2.3.3	All	All	All
Application	Rubyonrails	Rails	2.3.4	All	All	All
Application	Rubyonrails	Rails	2.3.9	All	All	All
Application	Rubyonrails	Rails	3.0.0	All	All	All
Application	Rubyonrails	Rails	3.0.0	beta	All	All
Application	Rubyonrails	Rails	3.0.0	beta2	All	All
Application	Rubyonrails	Rails	3.0.0	beta3	All	All
Application	Rubyonrails	Rails	3.0.0	beta4	All	All
Application	Rubyonrails	Rails	3.0.0	rc	All	All
Application	Rubyonrails	Rails	3.0.0	rc2	All	All
Application	Rubyonrails	Rails	3.0.1	All	All	All
Application	Rubyonrails	Rails	3.0.1	pre	All	All
Application	Rubyonrails	Rails	3.0.10	All	All	All
Application	Rubyonrails	Rails	3.0.10	rc1	All	All
Application	Rubyonrails	Rails	3.0.11	All	All	All
Application	Rubyonrails	Rails	3.0.12	All	All	All
Application	Rubyonrails	Rails	3.0.12	rc1	All	All
Application	Rubyonrails	Rails	3.0.13	All	All	All
Application	Rubyonrails	Rails	3.0.13	rc1	All	All

Application	Rubyonrails	Rails	3.0.13	rc1	All	All
Application	Rubyonrails	Rails	3.0.14	All	All	All
Application	Rubyonrails	Rails	3.0.16	All	All	All
Application	Rubyonrails	Rails	3.0.17	All	All	All
Application	Rubyonrails	Rails	3.0.18	All	All	All
Application	Rubyonrails	Rails	3.0.19	All	All	All
Application	Rubyonrails	Rails	3.0.2	All	All	All
Application	Rubyonrails	Rails	3.0.2	pre	All	All
Application	Rubyonrails	Rails	3.0.20	All	All	All
Application	Rubyonrails	Rails	3.0.3	All	All	All
Application	Rubyonrails	Rails	3.0.4	rc1	All	All
Application	Rubyonrails	Rails	3.0.5	All	All	All
Application	Rubyonrails	Rails	3.0.5	rc1	All	All
Application	Rubyonrails	Rails	3.0.6	All	All	All
Application	Rubyonrails	Rails	3.0.6	rc1	All	All
Application	Rubyonrails	Rails	3.0.6	rc2	All	All
Application	Rubyonrails	Rails	3.0.7	All	All	All
Application	Rubyonrails	Rails	3.0.7	rc1	All	All
Application	Rubyonrails	Rails	3.0.7	rc2	All	All
Application	Rubyonrails	Rails	3.0.8	All	All	All
Application	Rubyonrails	Rails	3.0.8	rc1	All	All
Application	Rubyonrails	Rails	3.0.8	rc2	All	All
Application	Rubyonrails	Rails	3.0.8	rc3	All	All
Application	Rubyonrails	Rails	3.0.8	rc4	All	All
Application	Rubyonrails	Rails	3.0.9	All	All	All
Application	Rubyonrails	Rails	3.0.9	rc1	All	All
Application	Rubyonrails	Rails	3.0.9	rc2	All	All
Application	Rubyonrails	Rails	3.0.9	rc3	All	All
Application	Rubyonrails	Rails	3.0.9	rc4	All	All
Application	Rubyonrails	Rails	3.0.9	rc5	All	All
Application	Rubyonrails	Ruby On Rails	3.0.4	All	All	All
Application	Rubyonrails	Ruby On Rails	3.0.4	All	All	All
cpe:2.3:a:rubyonrails:rails:2.3.0:*****:.*						
cpe:2.3:a:rubyonrails:rails:2.3.1:*****:.*						
cpe:2.3:a:rubyonrails:rails:2.3.10:*****:.*						

cpe:2.3:a:rubyonrails:rails:2.3.11:****:*:*:
cpe:2.3:a:rubyonrails:rails:2.3.12:****:*:*:
cpe:2.3:a:rubyonrails:rails:2.3.13:****:*:*:
cpe:2.3:a:rubyonrails:rails:2.3.14:****:*:*:
cpe:2.3:a:rubyonrails:rails:2.3.15:****:*:*:
cpe:2.3:a:rubyonrails:rails:2.3.16:****:*:*:
cpe:2.3:a:rubyonrails:rails:2.3.2:****:*:*:
cpe:2.3:a:rubyonrails:rails:2.3.3:****:*:*:
cpe:2.3:a:rubyonrails:rails:2.3.4:****:*:*:
cpe:2.3:a:rubyonrails:rails:2.3.9:****:*:*:
cpe:2.3:a:rubyonrails:rails:3.0.0:****:*:*:
cpe:2.3:a:rubyonrails:rails:3.0.0:beta:****:*:*:
cpe:2.3:a:rubyonrails:rails:3.0.0:beta2:****:*:*:
cpe:2.3:a:rubyonrails:rails:3.0.0:beta3:****:*:*:
cpe:2.3:a:rubyonrails:rails:3.0.0:beta4:****:*:*:
cpe:2.3:a:rubyonrails:rails:3.0.0:rc:****:*:*:
cpe:2.3:a:rubyonrails:rails:3.0.0:rc2:****:*:*:
cpe:2.3:a:rubyonrails:rails:3.0.1:****:*:*:
cpe:2.3:a:rubyonrails:rails:3.0.1:pre:****:*:*:
cpe:2.3:a:rubyonrails:rails:3.0.10:****:*:*:
cpe:2.3:a:rubyonrails:rails:3.0.10:rc1:****:*:*:
cpe:2.3:a:rubyonrails:rails:3.0.11:****:*:*:
cpe:2.3:a:rubyonrails:rails:3.0.12:****:*:*:
cpe:2.3:a:rubyonrails:rails:3.0.12:rc1:****:*:*:
cpe:2.3:a:rubyonrails:rails:3.0.13:****:*:*:
cpe:2.3:a:rubyonrails:rails:3.0.13:rc1:****:*:*:
cpe:2.3:a:rubyonrails:rails:3.0.14:****:*:*:
cpe:2.3:a:rubyonrails:rails:3.0.16:****:*:*:
cpe:2.3:a:rubyonrails:rails:3.0.17:****:*:*:

```
cpe:2.3:a:rubyonrails:rails:3.0.17::: : : : : : :
```

```
cpe:2.3:a:rubyonrails:rails:3.0.18:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.19:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.2:pre:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.20:*:*:*:*:*:*:
```

cpe:2.3:a:rubyonrails:rails:3.0.3:*:*:*:*:*:*:

```
cpe:2.3:a:rubyonrails:rails:3.0.4:rc1:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.5:rc1:*:*:*:*:*:
```

cpe:2.3:a:rubyonrails:rails:3.0.6:*:*:*:*:*:

```
cpe:2.3:a:rubyonrails:rails:3.0.6:rc1:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.6:rc2:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.7:rc1:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.7:rc2:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.8:rc1:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.8:rc2:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.8:rc3:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.8:rc4:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.9:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.9:rc1:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.9:rc2:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.9:rc3:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:3.0.9:rc4:*:*:*:*:*:
```

cpe:2.3:a:rubyonrails:rails:3.0.9:rc5:*:*:*:*:*:

```
cpe:2.3:a:rubyonrails:rails:2.3.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:rubyonrails:rails:2.3.1:*:*:*:*:*:*:
```

cpe:2.3:a:rubyonrails:rails:2.3.10:*****:
cpe:2.3:a:rubyonrails:rails:2.3.11:*****:
cpe:2.3:a:rubyonrails:rails:2.3.12:*****:
cpe:2.3:a:rubyonrails:rails:2.3.13:*****:
cpe:2.3:a:rubyonrails:rails:2.3.14:*****:
cpe:2.3:a:rubyonrails:rails:2.3.15:*****:
cpe:2.3:a:rubyonrails:rails:2.3.16:*****:
cpe:2.3:a:rubyonrails:rails:2.3.2:*****:
cpe:2.3:a:rubyonrails:rails:2.3.3:*****:
cpe:2.3:a:rubyonrails:rails:2.3.4:*****:
cpe:2.3:a:rubyonrails:rails:2.3.9:*****:
cpe:2.3:a:rubyonrails:rails:3.0.0:*****:
cpe:2.3:a:rubyonrails:rails:3.0.0:beta:*****:
cpe:2.3:a:rubyonrails:rails:3.0.0:beta2:*****:
cpe:2.3:a:rubyonrails:rails:3.0.0:beta3:*****:
cpe:2.3:a:rubyonrails:rails:3.0.0:beta4:*****:
cpe:2.3:a:rubyonrails:rails:3.0.0:rc:*****:
cpe:2.3:a:rubyonrails:rails:3.0.0:rc2:*****:
cpe:2.3:a:rubyonrails:rails:3.0.1:*****:
cpe:2.3:a:rubyonrails:rails:3.0.1:pre:*****:
cpe:2.3:a:rubyonrails:rails:3.0.10:*****:
cpe:2.3:a:rubyonrails:rails:3.0.10:rc1:*****:
cpe:2.3:a:rubyonrails:rails:3.0.11:*****:
cpe:2.3:a:rubyonrails:rails:3.0.12:*****:
cpe:2.3:a:rubyonrails:rails:3.0.12:rc1:*****:
cpe:2.3:a:rubyonrails:rails:3.0.13:*****:
cpe:2.3:a:rubyonrails:rails:3.0.13:rc1:*****:
cpe:2.3:a:rubyonrails:rails:3.0.14:*****:

cpe:2.3:a:rubyonrails:rails:3.0.16:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.17:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.18:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.19:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.2:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.2:pre:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.20:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.3:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.4:rc1:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.5:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.5:rc1:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.6:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.6:rc1:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.6:rc2:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.7:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.7:rc1:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.7:rc2:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.8:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.8:rc1:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.8:rc2:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.8:rc3:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.8:rc4:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.9:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.9:rc1:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.9:rc2:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.9:rc3:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.9:rc4:~::~::~:
cpe:2.3:a:rubyonrails:rails:3.0.9:rc5:~::~::~:
cpe:2.3:a:rubyonrails:ruby_on_rails:3.0.4:~::~::~:

cpe:2.3:a:rubyonrails:ruby_on_rails:3.0.4:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

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](#).

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