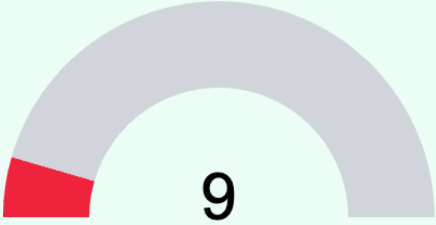
railsup

Report for upgradation of Rails from 4.0.0 to 8.0

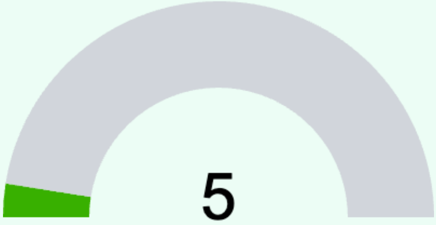
Success! Your Rails 4.0.0 to 8.0 Upgrade Report is Ready. The estimated time to upgrade your project is 14 weeks.

64	44	100
Vulnerabilities	Incompatibility	Rails Severity

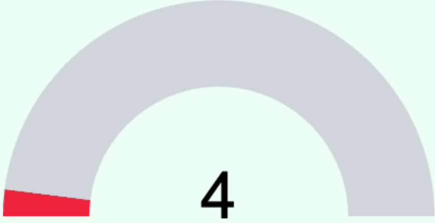
Overview



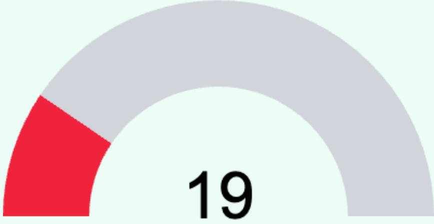
Outdated Gems



Compatible Gems

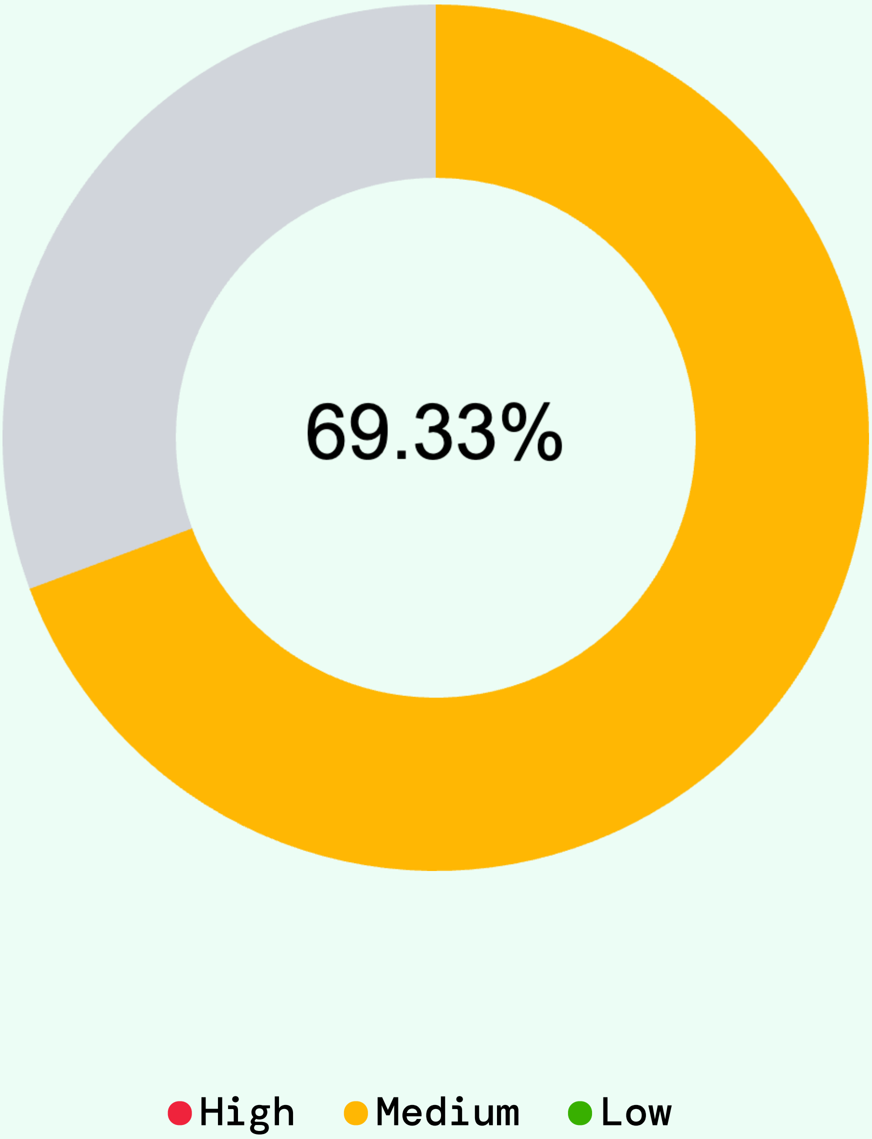


Incompatible Gems



Vulnerabilities

Complexity Level



Outdated Gems

#	Gem name	Installed Version	Latest Version
1	devise	3.1.1	4.9.4
2	mocha	0.13.3	2.7.1
3	mongoid	4.0.0	9.0.3
4	omniauth	1.0.3	2.1.2
5	omniauth-facebook	1.4.0	10.0.0
6	omniauth-oauth2	1.0.3	1.8.0
7	omniauth-openid	1.0.1	2.0.1
8	rdoc	4.0.1	6.10.0
9	sqlite3	1.3.7	2.5.0

Compatible Report

#	Gem name	Compatible
1	devise	✕
2	mocha	✓
3	mongoid	✓
4	omniauth	✓
5	omniauth-facebook	✓
6	omniauth-oauth2	✕
7	omniauth-openid	✕
8	rdoc	✓
9	sqlite3	✕

Vulnerability Report

#	Name	Installed Ver	Possibility	Criticality
1	activerecord	4.0.0	Possible RCE escalation bug with Serialized Columns in Active Record	critical
2	activesupport	4.0.0	Potentially unintended unmarshalling of user-provided objects in MemCacheStore and RedisCacheStore	critical
3	devise	3.1.1	Devise Gem for Ruby Time-of-check Time-of-use race condition with lockable module	critical
4	nokogiri	1.5.9	Nokogiri gem contains several vulnerabilities in libxml2 and libxslt	critical
5	omniauth	1.0.3	OmniAuth's `lib/omniauth/failure_endpoint.rb` does not escape `message_key` value	critical
6	rack	1.5.2	Possible shell escape sequence injection vulnerability in Rack	critical
7	ruby-openid	2.2.3	ruby-openid SSRF via claimed_id request	critical
8	actionpack	4.0.0	Object leak vulnerability for wildcard controller routes in Action Pack	high
9	i18n	0.6.5	i18n Gem for Ruby lib/i18n/core_ext/hash.rb Hash#slice() Function Hash Handling DoS	high
10	json	1.8.0	json Gem for Ruby Unsafe Object Creation Vulnerability (additional fix)	high
11	moped	1.5.1	Data Injection Vulnerability in moped Rubygem	high
12	omniauth-facebook	1.4.0	omniauth-facebook Gem for Ruby Insecure Access Token Handling Authentication Bypass	high

13	rake	10.1.0	OS Command Injection in Rake	high
14	rdoc	4.0.1	RDoc OS command injection vulnerability	high
15	sprockets	2.10.0	Path Traversal in Sprockets	high
16	tzinfo	0.3.37	TZInfo relative path traversal vulnerability allows loading of arbitrary files	high
17	mail	2.5.4	CVE-2015-9097 rubygem-mail: SMTP injection via recipient email addresses	medium
18	omniauth-oauth2	1.0.3	Ruby on Rails omniauth-oauth2 Gem CSRF vulnerability	medium
19	rails	4.0.0	Rails vulnerable to Cross-site Scripting	medium

Disclaimer: * The findings and estimates provided in this report are based on the information available at the time of analysis and the predefined parameters of the tool. While every effort has been made to ensure accuracy, actual migration outcomes may vary due to unforeseen challenges, unique application configurations, or changes in project scope. Users are advised to use these insights as a guideline and perform thorough testing and validation before implementation.