



CVE-2015-7579

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2015-7579 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2016-02-16 02:59:00 UTC |
| Updated | 2019-08-08 15:16:00 UTC |
| Description | Cross-site scripting (XSS) vulnerability in the rails-html-sanitizer gem 1.0.2 for Ruby on Rails 4.2.x and 5.x allows remote at |

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|-------------|----------------|---------|--------|---------|----------|
| Application | Rubyonrails | Html Sanitizer | All | All | All | All |
| Application | Rubyonrails | Rails | 4.2.0 | All | All | All |
| Application | Rubyonrails | Rails | 4.2.0 | beta1 | All | All |
| Application | Rubyonrails | Rails | 4.2.0 | beta2 | All | All |
| Application | Rubyonrails | Rails | 4.2.0 | beta3 | All | All |
| Application | Rubyonrails | Rails | 4.2.0 | beta4 | All | All |
| Application | Rubyonrails | Rails | 4.2.0 | rc1 | All | All |
| Application | Rubyonrails | Rails | 4.2.0 | rc2 | All | All |
| Application | Rubyonrails | Rails | 4.2.0 | rc3 | All | All |
| Application | Rubyonrails | Rails | 4.2.1 | All | All | All |
| Application | Rubyonrails | Rails | 4.2.1 | rc1 | All | All |
| Application | Rubyonrails | Rails | 4.2.1 | rc2 | All | All |
| Application | Rubyonrails | Rails | 4.2.1 | rc3 | All | All |
| Application | Rubyonrails | Rails | 4.2.1 | rc4 | All | All |
| Application | Rubyonrails | Rails | 4.2.2 | All | All | All |
| Application | Rubyonrails | Rails | 4.2.3 | All | All | All |
| Application | Rubyonrails | Rails | 4.2.3 | rc1 | All | All |

| | | | | | | |
|-------------|-----------------------------|-----------------------|---------|---------|-----|-----|
| Application | Rubyonrails | Rails | 4.2.4 | All | All | All |
| Application | Rubyonrails | Rails | 4.2.4 | rc1 | All | All |
| Application | Rubyonrails | Rails | 4.2.5 | All | All | All |
| Application | Rubyonrails | Rails | 4.2.5 | rc1 | All | All |
| Application | Rubyonrails | Rails | 4.2.5 | rc2 | All | All |
| Application | Rubyonrails | Rails | 4.2.5.1 | All | All | All |
| Application | Rubyonrails | Rails | 4.2.5.2 | All | All | All |
| Application | Rubyonrails | Rails | 4.2.6 | rc1 | All | All |
| Application | Rubyonrails | Rails | 5.0.0 | beta1 | All | All |
| Application | Rubyonrails | Rails | 5.0.0 | beta1.1 | All | All |
| Application | Rubyonrails | Rails | 5.0.0 | beta2 | All | All |
| Application | Rubyonrails | Rails | 5.0.0 | beta3 | All | All |
| Application | Rubyonrails | Rails | 4.2.0 | All | All | All |
| Application | Rubyonrails | Rails | 4.2.0 | beta1 | All | All |
| Application | Rubyonrails | Rails | 4.2.0 | beta2 | All | All |
| Application | Rubyonrails | Rails | 4.2.0 | beta3 | All | All |
| Application | Rubyonrails | Rails | 4.2.0 | beta4 | All | All |
| Application | Rubyonrails | Rails | 4.2.0 | rc1 | All | All |
| Application | Rubyonrails | Rails | 4.2.0 | rc2 | All | All |
| Application | Rubyonrails | Rails | 4.2.0 | rc3 | All | All |
| Application | Rubyonrails | Rails | 4.2.1 | All | All | All |
| Application | Rubyonrails | Rails | 4.2.1 | rc1 | All | All |
| Application | Rubyonrails | Rails | 4.2.1 | rc2 | All | All |
| Application | Rubyonrails | Rails | 4.2.1 | rc3 | All | All |
| Application | Rubyonrails | Rails | 4.2.1 | rc4 | All | All |
| Application | Rubyonrails | Rails | 4.2.2 | All | All | All |
| Application | Rubyonrails | Rails | 4.2.3 | All | All | All |
| Application | Rubyonrails | Rails | 4.2.3 | rc1 | All | All |
| Application | Rubyonrails | Rails | 4.2.4 | All | All | All |
| Application | Rubyonrails | Rails | 4.2.4 | rc1 | All | All |
| Application | Rubyonrails | Rails | 4.2.5 | All | All | All |
| Application | Rubyonrails | Rails | 4.2.5 | rc1 | All | All |
| Application | Rubyonrails | Rails | 4.2.5 | rc2 | All | All |
| Application | Rubyonrails | Rails | 4.2.5.1 | All | All | All |
| Application | Rubyonrails | Rails | 4.2.5.2 | All | All | All |

| | | | | | | |
|-------------|-----------------------------|-----------------------|-------|---------|-----|-----|
| Application | Rubyonrails | Rails | 4.2.6 | rc1 | All | All |
| Application | Rubyonrails | Rails | 5.0.0 | beta1 | All | All |
| Application | Rubyonrails | Rails | 5.0.0 | beta1.1 | All | All |
| Application | Rubyonrails | Rails | 5.0.0 | beta2 | All | All |
| Application | Rubyonrails | Rails | 5.0.0 | beta3 | All | All |

References

Reference

[ruby-security-ann] 20160125 [CVE-2015-7579] XSS vulnerability in rails-html-sanitizer

Do not unescape already escaped HTML entities · rails/rails-html-sanitizer@49dfc15 · GitHub

[security-announce] openSUSE-SU-2016:0356-1: important: Security update

Rails Multiple Bugs Let Remote Users Determine Passwords, Modify Records, Bypass Security Restrictions, Deny Service, and Conduct Cross

[security-announce] SUSE-SU-2016:1146-1: important: Security update for

[SECURITY] Fedora 22 Update: rubygem-rails-html-sanitizer-1.0.1-2.fc22

[SECURITY] Fedora 23 Update: rubygem-rails-html-sanitizer-1.0.3-1.fc23

[security-announce] SUSE-SU-2016:0391-1: important: Security update for

oss-security - [CVE-2015-7579] XSS vulnerability in rails-html-sanitizer

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#)