



# CVE-2015-7580

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

## Summary

<b>CVE</b>	CVE-2015-7580
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-02-16 02:59:00 UTC
<b>Updated</b>	2019-08-08 15:16:00 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in lib/rails/html/scrubbers.rb in the rails-html-sanitizer gem before 1.0.3 for Ruby on R

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Rubyonrails</a>	<a href="#">Html Sanitizer</a>	All	All	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.0	All	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.0	beta1	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.0	beta2	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.0	beta3	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.0	beta4	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.0	rc1	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.0	rc2	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.0	rc3	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.1	All	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.1	rc1	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.1	rc2	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.1	rc3	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.1	rc4	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.2	All	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.3	All	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.3	rc1	All	All

Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.4	All	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.4	rc1	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.5	All	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.5	rc1	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.5	rc2	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.5.1	All	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.5.2	All	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.6	rc1	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	5.0.0	beta1	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	5.0.0	beta1.1	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	5.0.0	beta2	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	5.0.0	beta3	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.0	All	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.0	beta1	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.0	beta2	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.0	beta3	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.0	beta4	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.0	rc1	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.0	rc2	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.0	rc3	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.1	All	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.1	rc1	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.1	rc2	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.1	rc3	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.1	rc4	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.2	All	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.3	All	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.3	rc1	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.4	All	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.4	rc1	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.5	All	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.5	rc1	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.5	rc2	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.5.1	All	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.5.2	All	All	All

Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	4.2.6	rc1	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	5.0.0	beta1	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	5.0.0	beta1.1	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	5.0.0	beta2	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	5.0.0	beta3	All	All

## References

### Reference

convert CDATA nodes to TEXT nodes to avoid XSS issues · rails/rails-html-sanitizer@63903b0 · 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

[rubyonrails-security] 20160125 [CVE-2015-7580] Possible XSS vulnerability in rails-html-sanitizer

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

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

oss-security - [CVE-2015-7580] Possible 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](#)