Redmine - Defect #38875

Additional vulnerabilities reported for v.5.0.5

2023-07-23 06:45 - A Fora

Status:	Needs feedback	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:			
Resolution:		**Affected version:**	5.0.5

Description

In version 5.0.5:

```
Name: actionpack
Version: 6.1.7.2
CVE: CVE-2023-28362
GHSA: GHSA-4g8v-vg43-wpgf
Criticality: Unknown
URL: https://discuss.rubyonrails.org/t/cve-2023-28362-possible-xss-via-user-supplied-values-to-redirect-to/83132
Title: Possible XSS via User Supplied Values to redirect_to
Solution: upgrade to '~> 6.1.7.4', '>= 7.0.5.1'

Name: actionview
Version: 6.1.7.2
CVE: CVE-2023-23913
GHSA: GHSA-xp5h-f8jf-rc8q
Criticality: High
URL: https://discuss.rubyonrails.org/t/cve-2023-23913-dom-based-cross-site-scripting-in-rails-ujs-for-contenteditable-html-elements/82468
Title: DOM Based Cross-site Scripting in rails-ujs for contenteditable HTML Elements
Solution: upgrade to '~> 6.1.7.3', '>= 7.0.4.3'

Name: commonmarker
Version: 0.23.8
GHSA: GHSA-48wp-p9qv-4j64
Criticality: High
URL: https://github.com/gjtorikian/commonmarker/releases/tag/v0.23.9
Title: Commonmarker vulnerable to to several quadratic complexity bugs that may lead to denial of service
Solution: upgrade to '>= 0.23.9'

Name: rack
Version: 2.2.6.3
CVE: CVE-2023-27539
GHSA: GHSA-c6qg-cjj8-47qp
Criticality: Unknown
URL: https://discuss.rubyonrails.org/t/cve-2023-27539-possible-denial-of-service-vulnerability-in-racks-header-parsing/82466
Title: Possible Denial of Service Vulnerability in Rack’s header parsing
Solution: upgrade to '~> 2.0, >= 2.2.6.4', '>= 3.0.6.1'

Name: sanitize
Version: 6.0.1
CVE: CVE-2023-36823
GHSA: GHSA-f5ww-cq3m-q3g7
Criticality: High
URL: https://github.com/rgrove/sanitize/releases/tag/v6.0.2
Title: Sanitize vulnerable to Cross-site Scripting via insufficient neutralization  of `style` element content
Solution: upgrade to '>= 6.0.2'
```

Related issues:	
Related to Redmine - Patch #38374: Update Rails to 6.1.7.6	**Closed**

History

#1 - 2023-08-11 08:08 - Go MAEDA

- Related to Patch #38374: Update Rails to 6.1.7.6 added

#2 - 2023-10-23 04:33 - Mischa The Evil

- Affected version changed from 5.0.4 to 5.0.5

#3 - 2023-10-29 22:09 - Marius BĂLTEANU

- Status changed from New to Needs feedback

Can you rerun the security tests on 5.0.6?

#4 - 2024-05-06 20:47 - Marius BĂLTEANU

- Description updated