Redmine - Defect #33334

bump i18n for advisory: CVE-2014-10077

2020-04-21 16:37 - Popa Marius

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Fixed	**Affected version:**	4.0.7

Description

Please update i18n from 0.7.0 to 0.8.0

```
 bundle-audit
Name: i18n
Version: 0.7.0
Advisory: CVE-2014-10077
Criticality: Unknown
URL: https://github.com/svenfuchs/i18n/pull/289
Title: i18n Gem for Ruby lib/i18n/core_ext/hash.rb Hash#slice() Function Hash Handling DoS
Solution: upgrade to >= 0.8.0

Vulnerabilities found!
```

Related issues:

Related to Redmine - Feature #29946: Update i18n gem (~> 1.6.0)	**Closed**

History

#1 - 2020-04-22 07:23 - Go MAEDA

- Related to Feature #29946: Update i18n gem (~> 1.6.0) added

#2 - 2020-04-22 07:50 - Go MAEDA

Thank you for reporting the issue. The quickest workaround is to update to Redmine 4.1. Redmine 4.1 uses i18n 1.6.

source:/tags/4.1.1/Gemfile#L17

#3 - 2020-04-24 11:39 - Popa Marius

Thanks we did it that way , also in 4.0.x branch i18n should be bumped to 0.8.0

#4 - 2020-04-24 13:20 - Marius BĂLTEANU

Popa Marius wrote:

> Thanks we did it that way , also in 4.0.x branch i18n should be bumped to 0.8.0

Is not only the bump, it requires also to backport some code changes from r17888 and r18286. At that time, Toshi tried to update the gem https://www.redmine.org/projects/redmine/repository/revisions/16324.

#5 - 2020-04-27 14:47 - Holger Just

The version of Hash#slice in the i18n gem (which was vulnerable to CVE-2014-10077) is only used if there is not already another version of this method present:

- From Ruby 2.5.0 on, Ruby itself ships this method.
- When used with Rails (resp. ActiveSupport) on version >= 3.0, < 6.0, it also ships this method. It is used in preference to the one in the i18n gem since ActiveSupport is loaded before i18n

Thus, the version of the method shipped with the i18n gem should never actually be used by us (or any dependent code). Thus, I think this vulnerability doesn't apply to us.

#6 - 2021-04-10 08:27 - Go MAEDA

- Status changed from New to Closed

- Resolution set to Fixed

Currently, all supported versions of Redmine (4.1 and 4.2) use i18n 1.6 or higher.

source:tags/4.2.0/Gemfile#L17
source:tags/4.1.2/Gemfile#L17