Redmine - Defect #26183

Use Nokogiri 1.7.2

2017-06-17 11:45 - Go MAEDA

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Jean-Philippe Lang	**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.2.7		
Resolution:	Fixed	**Affected version:**	3.2.6

Description

Redmine 3.3-stable / 3.2-stable uses Nokogiri 1.6.8 but version from 1.6.8 from 1.7.1 has some security issues (see https://github.com/sparklemotion/nokogiri/blob/master/CHANGELOG.md for details).

Fixed in 1.7.2:

- CVE-2017-5029
- CVE-2016-4738

Fixed in 1.7.1:

- CVE-2016-4658
- CVE-2016-5131

We should use Nokogiri >= 1.7.2 but unfortunately it requires Ruby >= 2.1.0 (see r16167). The attached patch uses Nokogiri ~> 1.7.2 if RUBY_VERSION >= 2.1.0.

I received this report from Sho Hashimoto.

Related issues:

Related to Redmine - Feature #25538: Drop support for Ruby 2.2.1 and ealier, ...	**Closed**
Related to Redmine - Defect #27505: Cannot install nokogiri 1.7 on Windows Ru...	**Closed**

Associated revisions

Revision 16676 - 2017-06-17 12:48 - Jean-Philippe Lang

Use Nokogiri 1.7.2 if possible (#26183).

Patch by Go MAEDA.

Revision 16683 - 2017-06-25 10:37 - Jean-Philippe Lang

Merged r16676 (#26183).

Revision 16684 - 2017-06-25 10:37 - Jean-Philippe Lang

Merged r16676 (#26183).

History

#1 - 2017-06-18 06:00 - Go MAEDA

- Target version set to 3.2.7

#2 - 2017-06-19 08:22 - Toshi MARUYAMA

- Project changed from 2 to Redmine

- Subject changed from Use Nokogiri 1.7.2 if possible to Nokogiri 1.7.2

- Category set to Security

#3 - 2017-06-19 08:23 - Toshi MARUYAMA

Backport USN-3235-1 to 1.6.8.x stream
https://github.com/sparklemotion/nokogiri/pull/1640

#4 - 2017-06-19 08:25 - Toshi MARUYAMA

- Related to Feature #25538: Drop support for Ruby 2.2.1 and ealier, 2.2.2+ is now required added

#5 - 2017-06-19 13:26 - Toshi MARUYAMA

Nokogiri team refused to maintain old release for old Ruby.
https://github.com/sparklemotion/nokogiri/pull/1640#issuecomment-309409944

#6 - 2017-06-19 15:01 - Holger Just

In that case, there is not much we can do, besides advising people that it might be a good idea to use a more modern Ruby. People who still require the use of older Rubies (e.g. because they can't or are not allowed to install newer versions) have to deal with the security implications this might bring. They can still use nokogiri 1.6.8 securely if they use a (patched) libxml version from their OS.

As for removing the support for older ruby versions: my comments in #25538 still stand.

#7 - 2017-06-25 10:37 - Jean-Philippe Lang

- Subject changed from Nokogiri 1.7.2 to Use Nokogiri 1.7.2

- Status changed from New to Closed

- Assignee set to Jean-Philippe Lang

- Resolution set to Fixed

#8 - 2017-11-25 20:43 - Toshi MARUYAMA

- Related to Defect #27505: Cannot install nokogiri 1.7 on Windows Ruby 2.4 added

Files

use-nokogiri-1_7_2.diff	429 Bytes	2017-06-17	Go MAEDA