# Redmine - Defect #9365
# Gravatar don't utilize HTTPS

2011-10-03 11:06 - Christian Speich

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 2011-10-03 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Jean-Baptiste Barth | **% Done:** | 0% |
| **Category:** | Accounts / authentication | **Estimated time:** | 0.00 hour |
| **Target version:** | | | |
| **Resolution:** | Wont fix | **Affected version:** | |

**Description**

When I set the scheme to https in the configuration and access my redmine installation via https, gravatars are not embedded via https. This may open security issues.

About your application's environment
Ruby version 1.8.7 (x86_64-linux)
RubyGems version 1.3.7
Rack version 1.1.2
Rails version 2.3.11
Active Record version 2.3.11
Active Resource version 2.3.11
Action Mailer version 2.3.11
Active Support version 2.3.11
Application root /var/www-vhosts/redmine-christian-speich/redmine
Environment production
Database adapter mysql
Database schema version 20110511000000

**Related issues:**

| | | |
|---|---|---|
| Related to Redmine - Patch # 5929: https-enabled gravatars when called over h... | **Closed** | **2010-07-21** |
| Related to Redmine - Patch # 18911: check Setting.protocol when determining g... | **Closed** | |
| Related to Redmine - Defect # 21855: Gravatar get images over http instead https | **Closed** | |

## Associated revisions

**Revision 10184 - 2012-08-09 20:04 - Jean-Philippe Lang**

Use SSL for gravatars according to the protocol in settings (#9365).

**Revision 10186 - 2012-08-10 18:35 - Jean-Philippe Lang**

Reverted r10184 (#9365).

## History

**#1 - 2011-10-03 13:59 - Etienne Massip**

*- Category set to Accounts / authentication*

**#2 - 2012-07-31 12:31 - Jean-Baptiste Barth**

*- Status changed from New to Confirmed*

*- Assignee set to Jean-Baptiste Barth*

*- Target version set to Candidate for next major release*

*- Affected version (unused) changed from 1.2.1 to devel*
*- Affected version deleted (1.2.1)*

Still a problem on Redmine 2.x, and it's a problem for me too as Chrome issues a certificate error because of that.

Analysis: In fact in turns out that the gravatar URL scheme (http or https) does not depend on the "http/https" option in the first tab. It depends on wether your request is run in SSL mode or not. See here in the code. If your Redmine runs behind a reverse-proxy, with this kind of architecture: HTTPS->RP->HTTP->APP_SERVER, the application server thinks it runs in HTTP mode while your clients access Redmine in HTTPS mode.

Proposal: I think we should rely on the "HTTP/HTTPS" setting on the first page, and do not make assumptions on how Redmine is hosted.

Etienne or Jean-Philippe: let me know what you think, I'll take care of this issue if we agree on the proposal.

#### #3 - 2012-07-31 13:33 - Toshi MARUYAMA

gravatar embedded Redmine is obsolete.

- source:tags/2.0.3/lib/plugins/gravatar
- https://github.com/woods/gravatar-plugin

Should we change to gravatarify?
https://www.chiliproject.org/issues/1033

#### #4 - 2012-08-09 17:02 - Jean-Philippe Lang

*- Target version changed from Candidate for next major release to 2.0.4*

Jean-Baptiste Barth wrote:

> *Proposal: I think we should rely on the "HTTP/HTTPS" setting on the first page, and do not make assumptions on how Redmine is hosted.*

Agreed.

Toshi MARUYAMA wrote:

> *Should we change to gravatarify?*

Is this change supposed to fix anything?

#### #5 - 2012-08-09 19:29 - Toshi MARUYAMA

Jean-Philippe Lang wrote:

> *Toshi MARUYAMA wrote:*
>
> > *Should we change to gravatarify?*

> *Is this change supposed to fix anything?*

Sorry, I misunderstood.
Changing avatar plugin has no effect to this issue.

#### #6 - 2012-08-09 20:05 - Jean-Philippe Lang

*- Status changed from Confirmed to Resolved*
*- Resolution set to Fixed*

Fix committed in r10184.

Toshi MARUYAMA wrote:

> *Sorry, I misunderstood.*
> *Changing avatar plugin has no effect to this issue.*

No problem, upgrading would be fine anyway.

#### #7 - 2012-08-10 04:28 - Levi Corcoran

I think r10184 will break the scenario where users optionally use SSL to access a Redmine installation. In our environment SSL is forced so it's not a concern personally, but you'll end up loading mixed content if the settings are configured for HTTP but a user explicitly makes an HTTPS request. This was previously reported in #5929.

It seems the ideal fix would load Gravatar images over SSL if either HTTPS is configured in Redmine settings, OR the current request is using HTTPS.

(Note: we did have to set Apache up to use X-Forwarded-Proto headers to get Gravatar images properly served over SSL through Thin, and r10184 would prevent that since we do have HTTPS configured in the Redmine settings - so that's an improvement for me, but I'm not sure how many folks may be using optional HTTPS and have similar concerns to those raised in #5929).

#### #8 - 2012-08-10 18:38 - Jean-Philippe Lang

*- Status changed from Resolved to Closed*
*- Target version deleted (2.0.4)*
*- Resolution changed from Fixed to Wont fix*

You're right, I've reverted r10184. X-Forwarded-Proto should be used instead, so I'm closing it.

#### #9 - 2012-08-10 21:50 - Jean-Baptiste Barth

Fine with that, I didn't know Rails (or Rack) was following X-Forwarded-Proto, thanks.

#### #10 - 2014-10-02 00:07 - Yannick Warnier

Hi, I'm using Redmine 2.4.1.stable with Protocol option set to HTTPS (and obviously use HTTPS itself to connect) and I have the issue of gravatar icons not being loaded in SSL.

As initially reported, this may open security issues. Apparently it was fixed 2 years ago, so I guess I am reporting some kind of regression.

#### #11 - 2015-02-03 16:25 - Toshi MARUYAMA

*- Related to Patch #18911: check Setting.protocol when determining gravatar protocol added*

#### #12 - 2015-02-03 16:33 - Toshi MARUYAMA

Yannick Warnier wrote:

> *Hi, I'm using Redmine 2.4.1.stable with Protocol option set to HTTPS (and obviously use HTTPS itself to connect) and I have the issue of gravatar icons not being loaded in SSL.*
>
> *As initially reported, this may open security issues. Apparently it was fixed 2 years ago, so I guess I am reporting some kind of regression.*

Did you try X-Forwarded-Proto?

#### #13 - 2016-02-08 13:58 - Go MAEDA

*- Related to Defect #21855: Gravatar get images over http instead https added*

#### #14 - 2016-04-08 10:58 - Yann Collette

Still a problem with version 3.2.0

#### #15 - 2016-04-09 01:19 - Toshi MARUYAMA

Yann Collette wrote:

> *Still a problem with version 3.2.0*

See #21855.