Redmine - Defect #35417

User sessions not reset after 2FA activation

2021-06-14 11:19 - Holger Just

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Go MAEDA	**% Done:**	0%
Category:	Accounts / authentication	**Estimated time:**	0.00 hour
Target version:	4.2.2		
Resolution:	Fixed	**Affected version:**	

Description

Felix Schäfer reports via email to security@redmine.org

> Hello,
>
> Currently a user signed up on multiple browsers/machines can activate 2FA in one session but still continue using the other sessions. This presents a security risk if an attacker has or gets control of one of those other sessions.
>
> The attached patch resets all the session, autologin and recovery keys of a user when 2FA is set up. Maybe a warning could also be added to the 2FA set up screen about this so that users with multiple active sessions are not surprised about getting logged out from the other sessions.
>
> Thank you,
>
> Felix Schäfer

Related issues:

Related to Redmine - Feature #1237: Add support for two-factor authentication	**Closed**	**2008-05-14**

Associated revisions

Revision 21069 - 2021-07-15 03:44 - Go MAEDA

User sessions not reset after 2FA activation (#35417).

Patch by Felix Schäfer.

Revision 21070 - 2021-07-17 09:39 - Go MAEDA

Merged r21069 from trunk to 4.2-stable (#35417).

Revision 21104 - 2021-07-28 17:59 - Marius BĂLTEANU

Adds test for #35417.

Revision 21107 - 2021-07-28 19:34 - Marius BĂLTEANU

Merged r21104 to 4.2-stable (#35417).

History

#1 - 2021-06-25 11:57 - Go MAEDA

- Target version set to 4.2.2

Setting the target version to 4.2.2.

> Maybe a warning could also be added to the 2FA set up screen about this so that users with multiple active sessions are not surprised about getting logged out from the other sessions.

Although it would be more user-friendly to display such a message, I think the patch can be merged as-is because Redmine currently don't show such warning when resseting session by timeout or some reasons.

#2 - 2021-06-25 17:47 - Holger Just

Go MAEDA wrote:

> Although it would be more user-friendly to display such a message, I think the patch can be merged as-is because Redmine currently don't show such warning when resseting session by timeout or some reasons.

I agree. We also destroy / logout other sessions on password change without any further warning. I think this can be merged as is.

#3 - 2021-07-15 03:44 - Go MAEDA

- Status changed from New to Resolved

- Assignee set to Go MAEDA

Committed the patch. Thank you.

#4 - 2021-07-17 09:39 - Go MAEDA

- Status changed from Resolved to Closed

#5 - 2021-07-20 14:37 - Holger Just

- Status changed from Closed to Reopened

- Assignee changed from Go MAEDA to Holger Just

Thank you Maeda-san.

As this is now comitted, I would go ahead and reserve a CVE-ID for this issue. The CVE-ID will be marked as reserved until we have a release containing this fix.

#6 - 2021-07-21 16:55 - Holger Just

CVE-2021-37156 was assigned for this.

The CVE entry is not yet public. Once we have a release with this fix, we have to update the CVE entry on https://cveform.mitre.org/ and add a reference to the news and the updated /Security_Advisories page.

#7 - 2021-07-26 12:26 - Marius BĂLTEANU

We can cut a release this weekend, is it ok?

#8 - 2021-07-26 12:56 - Holger Just

Sure!

#9 - 2021-07-27 23:00 - Marius BĂLTEANU

- Related to Feature #1237: Add support for two-factor authentication added

#10 - 2021-07-27 23:16 - Marius BĂLTEANU

- File test_for_35417.patch added

I've added a test for this case, Holger, can you take a look, please?

As Mischa mentioned in #35611, we should have this covered by tests.

#11 - 2021-07-28 11:58 - Holger Just

- Assignee deleted (Holger Just)

Thank you! I tested the test (heh) and it appears to work correctly (fails without the original patch, works with both in place). I think this one can be merged.

The second part of the patch is however still untested, namely that concurrent active sessions are destroyed if 2fa is activated. I'm not sure how we can properly test the handling of concurrent sessions though...

In any case, could you (Marius and Maeda-san) coordinate to merge this in time before the release?

#12 - 2021-07-28 12:07 - Marius BĂLTEANU

Holger Just wrote:

> Thank you! I tested the test (heh) and it appears to work correctly (fails without the original patch, works with both in place). I think this one can be merged.
>
> The second part of the patch is however still untested, namely that concurrent active sessions are destroyed if 2fa is activated. I'm not sure how we can properly test the handling of concurrent sessions though...
>
> In any case, could you (Marius and Maeda-san) coordinate to merge this in time before the release?

Yes, I can do it later today.

#13 - 2021-07-29 08:50 - Marius BĂLTEANU

- Status changed from Reopened to Closed

- Assignee set to Go MAEDA

Test committed.

#14 - 2021-07-29 18:00 - Holger Just

For the security scanner, I would then use the following definition after the release:

```
register(
  id:        '2021-08-01',
  category:  :privilege_escalation,
  severity:  :low,
  details:   'User sessions not reset after activation of two-factor authentication',
  ticket_id: '35417',
  cves:      ['CVE-2021-37156'],
  fixed_in:  ['< 4.2.0', '>= 4.2.2']
)
```

with the following title:

> User sessions not reset after activation of two-factor authentication

and description:

> When enabling two-factor authentication for a user's account, Redmine allows existing user sessions to continue, resulting in increased risk if an attacker has or gets control of one of those other sessions.

#15 - 2021-08-01 08:53 - Marius BĂLTEANU

- Tracker changed from Patch to Defect

#16 - 2021-08-02 12:50 - Marius BĂLTEANU

Holger Just wrote:

> For the security scanner, I would then use the following definition after the release:
>
> [...]
>
> with the following title:
>
> > User sessions not reset after activation of two-factor authentication
>
> and description:
>
> > When enabling two-factor authentication for a user's account, Redmine allows existing user sessions to continue, resulting in increased risk if an attacker has or gets control of one of those other sessions.

Thanks Holger for your feedback and also for your updates made today to the Wiki page. I saw that you updated the severity to Medium for this issue and then you reverted without any comment. Is it ok or you reverted by mistake?

#17 - 2021-08-02 13:08 - Holger Just

When updating the security scanner yesterday, I thought a bit more about the possible impact of this. After comparing it with other issues we had tagged as "low" in the past, I came to the conclusion that this probably deserved a medium. I initially tagged it in the security scanner as such.

Only after having updated the severity in the wiki page however, I saw that you mentioned the severity in the release news article as low. Unwilling to change it there too and convinced that consistency is more important than my hunch of severity, I reverted it everywhere back to low. Sorry for this back-and-forth :(

#18 - 2021-08-02 13:13 - Marius BĂLTEANU

Holger Just wrote:

> When updating the security scanner yesterday, I thought a bit more about the possible impact of this. After comparing it with other issues we had tagged as "low" in the past, I came to the conclusion that this probably deserved a medium. I initially tagged it in the security scanner as such.
>
> Only after having updated the severity in the wiki page however, I saw that you mentioned the severity in the release news article as low. Unwilling to change it there too and convinced that consistency is more important than my hunch of severity, I reverted it everywhere back to low. Sorry for this back-and-forth :(

Don't worry, I just wanted to double check this with you. In the future, I will avoid posting the severity in the news post.

#19 - 2021-08-03 18:00 - Holger Just

I have requested an update for CVE-2021-37156 on https://cveform.mitre.org/ with the following references:

- https://www.redmine.org/news/132
- https://www.redmine.org/projects/redmine/wiki/Security_Advisories

The CVE should be published in the next few hours with this new information.

#20 - 2022-06-21 08:12 - Marius BĂLTEANU

- Project changed from 2 to Redmine

- Category set to Accounts / authentication

- Resolution set to Fixed

Files

2fa-session-reset.patch	1.24 KB	2021-06-14	Holger Just
test_for_35417.patch	1.18 KB	2021-07-27	Marius BĂLTEANU