

41

Unauthenticated Private Messages Disclosure via wordpress Rest API

Share:



SUMMARY BY GHIMIRE_VESHRAJ



Tribute to Late [Internet Hero Binit](#) 🙏❤️

You were my source of inspiration and motivation. Though we can't see you or meet you, you will always stay alive and smiling in our memories and hearts. May your soul rest in peace. 🙏

Sensei LMS <= 4.4.3 - Unauthenticated Private Messages Disclosure via Rest API ([CVE-2022-2034](#))

The plugin does not have proper permissions set in one of its REST endpoint, allowing unauthenticated users to access private messages sent to teachers.

TIMELINE



[ghimire_veshraj](#) submitted a report to [Automattic](#).

Jun 3rd (6 months ago)

Vulnerable Plugin: Sensei LMS

Hi there,

Hope you are doing well,

So, i noticed that their is an option to contact teacher on Sensei LMS which is meant to private.

By default, other user can't see the question I asked to the teacher.

But using the `/wp-json/wp/v2/sensei-messages/<numericID>` where numeric ID can be bruteforced.

Those private questions asked to teacher is still visible to any Unauthenticated User.

Image F1754958: Screen_Shot_2022-06-03_at_10.08.45_AM.png 999.74 KiB

[Zoom in](#) [Zoom out](#) [Copy](#) [Download](#)



Steps to reproduce:

Create any course then as a student, ask question on that course.

Now, the message is visible through `/wp-json/wp/v2/sensei-messages/<numericID>`

Sensei LMS lacks authentication in a REST API endpoint, allowing unauthenticated users to discover private questions sent between teacher and student on the site.

Impact

Disclosure of Private Questions to Unauthenticated User.

1 attachment:

F1754958: [Screen_Shot_2022-06-03_at_10.08.45_AM.png](#)



xknown Automattic staff posted a comment.

Jun 3rd (6 months ago)

Thank you for your submission. Your report will be reviewed and we'll get back to you shortly.



[ghimire_veshraj](#) posted a comment.

Jun 6th (6 months ago)

Hi @xknown

Any updates?

Please let me know if you are having trouble in reproducing this.

Regards,

Veshraj Ghimire



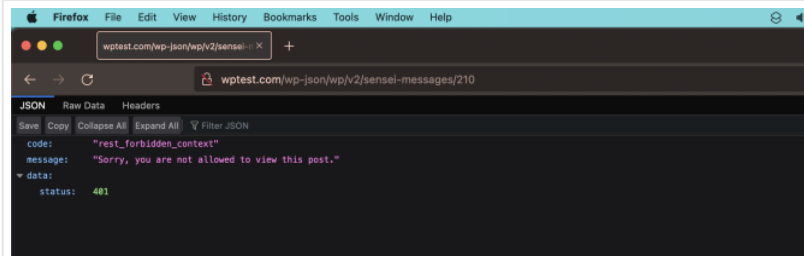
xknown Automatic staff changed the status to ○ **Triaged**.

Jun 6th (6 months ago)

Hi @ghimire_veshraj, there's no need for additional information. We confirmed the issue and we are already testing a potential fix for this issue.


ghimire_veshraj posted a comment.


Jun 16th (5 months ago)



1 attachment:

F1777623: [Screen_Shot_2022-06-17_at_7.26.04_AM.png](#)

 **xknown** Automatic staff closed the report and changed the status to Resolved. Jun 21st (5 months ago)
Hi [@ghimire_veshraj](#), thanks again for the report. As you already noticed, the sensei team released a fix for in the 4.5.0 version.

 **Automattic** rewarded [ghimire_veshraj](#) with a \$300 bounty and a \$50 bonus. Jun 21st (5 months ago)
Hi, we would like thank you again for your submission and helping make Automattic a safer place. We look forward to more reports from you in the future.

 [ghimire_veshraj](#) requested to disclose this report. Jun 21st (5 months ago)
Thank you so much for the bounty :)

 [ghimire_veshraj](#) posted a comment. Updated Jul 22nd (4 months ago)
Hi [@xknown](#)

can we disclose this if you are okay with that?
Since it is 1 month+ from the resolved date :)

Regards,
Veshraj Ghimire

 **xknown** Automatic staff agreed to disclose this report. Aug 4th (4 months ago)

 This report has been disclosed. Aug 4th (4 months ago)