

[Home](#)

Webchat history is accessible without authentication in FMS<= 7.42

#pandorafms #hacking #chathistory #cve

Last Modified: 2021.06.08.

cve-2020-8497

Technical Details

In Artica Pandora FMS 7.42, an unauthenticated attacker can read the chat history. The file is in JSON format and it contains user names, user IDs, private messages, and timestamps. (http://.../pandora_console/attachment/pandora_chat.log.json.txt)

Unfortunately there are live installations with this bug and the chat history is visible like this. I got in touch with the vendor and they fixed it in Pandora FMS 7.44.

Additional Content

Demo Video



© 2019-2022 Kamilló Matek (<FMIITx) All Rights Reserved