NVD DB Update

CVE-2024-7053 - Score: 9.0

Components:

openwebui open webui 0.3.8

Description:

A vulnerability in open-webui/open-webui version 0.3.8 allows an attacker with a user-level account to perform a session fixation attack. The session cookie for all users is set with the default ‘SameSite=Lax‘ and does not have the ‘Secure‘ flag enabled, allowing the session cookie to be sent over HTTP to a cross-origin domain. An attacker can exploit this by embedding a malicious markdown image in a chat, which, when viewed by an administrator, sends the admin’s session cookie to the attacker’s server. This can lead to a stealthy administrator account takeover, potentially resulting in remote code execution (RCE) due to the elevated privileges of administrator accounts.

Main problems:

79 "Improper Neutralization of Input During Web Page Generation (’Cross-site Scripting’)"