Authentic 2 - Development #76809

poser HttpOnly sur le cookie OPENED_SESSION_COOKIE_NAME

20 avril 2023 09:38 - Frédéric Péters

Statut:	Fermé	**Début:**	20 avril 2023
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

Pour un audit qui dit :

> L'absence de l'attribut HttpOnly, combinée à une vulnérabilité de Cross Site Scripting affectant l'application permettrait à un attaquant de récupérer le cookie de session via un code JavaScript malveillant.

(oui il ne s'agit pas d'un cookie de session etc. mais ça fera taire l'audit).

Révisions associées

Révision fa13b52a - 20 avril 2023 14:19 - Benjamin Dauvergne

misc: set secure and http-only for cookie 'cookie-test' (#76809)

Révision 670481b0 - 18 janvier 2024 17:27 - Benjamin Dauvergne

misc: make opened session cookie http only and secure (#76809)

Historique

#1 - 20 avril 2023 13:39 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#2 - 20 avril 2023 13:44 - Robot Gitea

- Statut changé de Nouveau à En cours

Benjamin Dauvergne (bdauvergne) a ouvert une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/42
- Titre : WIP: misc: make opened session cookie http only and secure (#76809)
- Modifications : https://git.entrouvert.org/entrouvert/authentic/pulls/42/files

#3 - 20 avril 2023 13:45 - Benjamin Dauvergne

Pour secure je reprendre la valeur de SESSION_COOKIE_SECURE (y pas de raison de faire moins bien) pour HttpOnly je met toujours vrai parce que je ne connais aucun usage de ce cookie en JS, supposons que nous n'en introduirons jamais.

#4 - 20 avril 2023 14:04 - Robot Gitea

- Statut changé de En cours à Solution proposée

#5 - 20 avril 2023 14:20 - Robot Gitea

Benjamin Dauvergne (bdauvergne) a ouvert une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/43
- Titre : misc: set secure and http-only for cookie 'cookie-test' (#76809)
- Modifications : https://git.entrouvert.org/entrouvert/authentic/pulls/43/files

#6 - 20 avril 2023 14:38 - Robot Gitea

- Statut changé de Solution proposée à Solution validée

Emmanuel Cazenave (ecazenave) a approuvé une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/43

#8 - 20 avril 2023 19:20 - Robot Gitea

- Statut changé de Solution validée à Résolu (à déployer)

Benjamin Dauvergne (bdauvergne) a mergé une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/43
- Titre : misc: set secure and http-only for cookie 'cookie-test' (#76809)
- Modifications : https://git.entrouvert.org/entrouvert/authentic/pulls/43/files

#9 - 21 avril 2023 08:14 - Transition automatique

- Statut changé de Résolu (à déployer) à Solution déployée

#10 - 25 juin 2023 04:42 - Transition automatique

Automatic expiration

#11 - 16 janvier 2024 17:26 - Robot Gitea

Benjamin Dauvergne (bdauvergne) a fermé une pull request sur Gitea concernant cette demande.

#12 - 16 janvier 2024 17:30 - Benjamin Dauvergne

- Statut changé de Fermé à Nouveau

C'est cookie-test qui a été traité dans le ticket poussé, pas le bon cookie.

#13 - 16 janvier 2024 21:37 - Robot Gitea

- Statut changé de Nouveau à En cours

Benjamin Dauvergne (bdauvergne) a commencé à travailler sur une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/42
- Titre : WIP: misc: make opened session cookie http only and secure (#76809)
- Modifications : https://git.entrouvert.org/entrouvert/authentic/pulls/42/files

#14 - 16 janvier 2024 21:37 - Robot Gitea

- Statut changé de En cours à Solution proposée

#15 - 18 janvier 2024 11:43 - Robot Gitea

- Statut changé de Solution proposée à En cours

Thomas NOËL (tnoel) a relu et demandé des modifications sur une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/42

#16 - 22 janvier 2024 09:49 - Benjamin Dauvergne

- Statut changé de En cours à Solution proposée

#17 - 22 janvier 2024 10:42 - Robot Gitea

- Statut changé de Solution proposée à Solution validée

Thomas NOËL (tnoel) a approuvé une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/42

#18 - 22 janvier 2024 10:43 - Robot Gitea

- Statut changé de Solution validée à Résolu (à déployer)

Benjamin Dauvergne (bdauvergne) a mergé une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/42
- Titre : misc: make opened session cookie http only and secure (#76809)
- Modifications : https://git.entrouvert.org/entrouvert/authentic/pulls/42/files

#19 - 22 janvier 2024 11:14 - Transition automatique

- Statut changé de Résolu (à déployer) à Solution déployée

#20 - 24 mars 2024 04:42 - Transition automatique

Automatic expiration