w.c.s. - Bug #90085

403 sur appel d'une action global paramétrée en API ouverte, en recette.

26 avril 2024 15:07 - Nicolas Roche

Statut:	Solution déployée	**Début:**	26 avril 2024
Priorité:	Normal	**Echéance:**	
Assigné à:	Frédéric Péters	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

Vu sur le connecteur Maélis.

```
In [25]: logs = ResourceLog.objects.filter(appname='toulouse-maelis', slug='maelis', message__cont
ains='/hooks')
In [26]: [(x.extra.get('response_headers', {}).get('date'), x.extra.get('response_content')) for x
 in logs1]
...
('Fri, 26 Apr 2024 12:19:49 GMT',
  '{"err": 1, "err_class": "Access denied", "err_desc": "insufficient roles"}'),
```

L'action globale est paramétrée avec :
https://demarches-parsifal.test.entrouvert.org/backoffice/workflows/131/global-actions/3/

```
Rôles requis pour déclencher via un appel HTTP : Aucun (API ouverte)
```

(comme en production où l'on n'a pas l'erreur)

Révisions associées

Révision a88ff444 - 28 avril 2024 08:10 - Frédéric Péters

workflows: consider empty list when checking for permission (#90085)

Historique

#1 - 26 avril 2024 15:07 - Nicolas Roche

- Assigné à mis à Nicolas Roche

(je creuse...)

#2 - 26 avril 2024 15:14 - Frédéric Péters

Le message "API ouverte" doit être faux, et il doit y avoir un contrôle d'accès, ça a peut-être évolué avec le temps mais ça serait une bonne chose, on ne veut pas d'API ouverte.

#3 - 26 avril 2024 15:20 - Frédéric Péters

En fait non, j'imagine que passerelle signe l'appel, et dans ce cas on contrôle ce qui est spécifié :

```
                if not ('_signed_calls' in self.trigger.roles and is_url_signed()):
                    raise errors.AccessForbiddenError('insufficient roles')
```

bref c'est "API ouverte mais il ne faut pas signer les appels pour que ça soit le cas", éventuellement ici le commentaire levé pourrait être différent pour le cas où il n'y a rien dans trigger.roles, si tu veux faire ce patch.

#4 - 26 avril 2024 15:35 - Nicolas Roche

- Statut changé de Nouveau à En cours

J'ai modifié le déclencheur pour prendre les appels signés aux API.
J'ai relancé le trigger et c'est passé.

(Je modifie la PROD en conséquence, merci Fred.)

#5 - 26 avril 2024 15:47 - Nicolas Roche

- Assigné à Nicolas Roche supprimé

J'ai mis à jour Allo-Toulouse également (en préventif, je n'aurais peut-être pas du)
https://demarches-montoulouse.test.entrouvert.org/backoffice/workflows/73/global-actions/17/
https://demarches-montoulouse.eservices.toulouse-metropole.fr/backoffice/workflows/91/global-actions/17/

(je regarde si je comprend tout bien avant de me lancer dans le patch)

#6 - 26 avril 2024 16:46 - Nicolas Roche

- Statut changé de En cours à Nouveau

J'abandonne ici.
Le code a changé avec #88875 et n'est plus vraiment adaptable pour préciser le message d'erreur.
Perso, j'aurais plutôt accepté les appels signés sur l'API ouverte, pour ne pas introduire de régression.

#7 - 26 avril 2024 17:24 - Frédéric Péters

> pour ne pas introduire de régression

Il faut préciser de quoi tu parles; veux-tu dire que le code de #88875 a modifié un comportement ?

#8 - 26 avril 2024 17:41 - Nicolas Roche

Non, #88875 n'était pas encore déployé quand j'ai ouvert ce ticket à propos de la régression (ici maelis, puis famille #90089).
Pardon d'embrouiller le ticket, je voulais juste dire que la version actuelle du code déporte la détection des erreurs
et que je ne me voyais pas ajouter la détection d'un cas d'erreur en dehors.

```
        if not self.trigger.check_executable(self.formdata, user):
            raise errors.AccessForbiddenError('insufficient roles')
```

#9 - 26 avril 2024 17:43 - Frédéric Péters

> ticket à propos de la régression

pourquoi parles-tu de régression, quel moment as-tu identifié où c'était ok et puis plus ok ?

#10 - 26 avril 2024 17:50 - Nicolas Roche

J'ai reçu dans les traces la 403 (que j'aurais du noter dans le ticket).
https://sentry.entrouvert.org/entrouvert/publik/issues/124145/
C'était la même que celle donnée dans #90089.

En recette les appels aux triggers qui passaient avant ne passeraient plus.
https://sentry.entrouvert.org/entrouvert/publik/issues/?query=hook
En prod, ça passe encore.

(édit: à quel moment -> Apr 26, 2024 11:19:43 AM UTC)

#11 - 26 avril 2024 17:57 - Frédéric Péters

> https://sentry.entrouvert.org/entrouvert/publik/issues/124145/

Il est marqué que ça commence "April 26 2024 13:19:43 CEST"; la release contenant #88875 (et autres) est tagguée à 11:11, déployée un peu après (notée déployée par scrutiny à 12:17.

> Non, #88875 n'était pas encore déployé

Tu es vraiment sûr ?

#12 - 26 avril 2024 18:02 - Nicolas Roche

Non, pardon. Je n'avais pas l'info de scrutiny
(et je n'ai pas reproduis pour pouvoir trouver le commit qui introduirait la régression).

#13 - 26 avril 2024 18:03 - Frédéric Péters

Bref, c'est sans doute bel et bien #88875, qui remplace :

```
-         if self.trigger.roles:
(...)
+         if self.roles is None:
+             return True
```

et ça doit passer à côté du cas liste vide.

#14 - 26 avril 2024 18:04 - Frédéric Péters

> Je n'avais pas l'info de scrutiny.

C'est l'heure à laquelle #88875#note-8, le ticket en question est marqué déployé.

#15 - 26 avril 2024 18:06 - Robot Gitea

- Statut changé de Nouveau à En cours

- Assigné à mis à Frédéric Péters

Frédéric Péters (fpeters) a ouvert une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/wcs/pulls/1444
- Titre : WIP: workflows: consider empty list when checking for permission (#90085)
- Modifications : https://git.entrouvert.org/entrouvert/wcs/pulls/1444/files

#16 - 26 avril 2024 19:19 - Robot Gitea

- Statut changé de En cours à Solution proposée

#17 - 27 avril 2024 22:41 - Robot Gitea

- Statut changé de Solution proposée à Solution validée

Lauréline Guérin (lguerin) a approuvé une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/wcs/pulls/1444

#18 - 28 avril 2024 08:10 - Robot Gitea

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

Frédéric Péters (fpeters) a mergé une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/wcs/pulls/1444
- Titre : workflows: consider empty list when checking for permission (#90085)
- Modifications : https://git.entrouvert.org/entrouvert/wcs/pulls/1444/files

#19 - 28 avril 2024 09:17 - Transition automatique

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