

w.c.s. - Bug #38240

Problème sur la clé signature des services en python3

05 décembre 2019 17:56 - Emmanuel Cazenave

Statut:	Fermé	Début:	05 décembre 2019
Priorité:	Normal	Echéance:	
Assigné à:	Emmanuel Cazenave	% réalisé:	0%
Catégorie:		Temps estimé:	0:00 heure
Version cible:		Planning:	Non
Patch proposed:	Oui		

Description

Problème de base un appel de wcs (qui tourne chez moi en py3) vers chrono qui échoue avec 'Invalid signature'.
En opération préalable j'avais shooté mon tenant chrono (parce que je m'en sortais pas de la contrainte d'unicité sur le slug des évènements), puis re-crédation via cook.

Dans le site-option.cfg :

```
[wscall-secrets]
....
chrono.dev.publik.love = a729046aa4faca7d5a4ae2fdee30551cab8d9d7caae4f830004d589575a1240
```

Retour à python2 pour wcs, déclenchement d'un check_hobo en ajoutant une variable coté hobo. Plus de problème d'appels vers chrono et dans site-options.cfg, la clé avec un caractère en plus :

```
[wscall-secrets]
....
chrono.dev.publik.love = a729046aa4faca7d5a4ae2fdee30551cab8d9d7caae4f830004d589575a1240c
```

Révisions associées

Révision e80f55d6 - 09 décembre 2019 09:48 - Emmanuel Cazenave

ctl: preserve key length in py3 (#38240)

Historique

#1 - 05 décembre 2019 18:16 - Emmanuel Cazenave

Et donc c'est check_hobos::shared_secret, avec en python2, le int(secret1, 16) qui retourne un long (<https://docs.python.org/2/library/functions.html#long>), dont la représentation hexadécimale se termine par un 'L', qui est volontairement shooté par :

```
return hex(int(secret1, 16) ^ int(secret2, 16))[2:-1]
<pre>
```

Mais en python3, plus de long, que des int, plus de 'L' à la fin, et plouf un caractère en moins dans la clé.

#2 - 05 décembre 2019 18:45 - Emmanuel Cazenave

- Fichier 0001-ctl-preserve-key-length-in-py3-38240.patch ajouté
- Statut changé de Nouveau à Solution proposée
- Assigné à mis à Emmanuel Cazenave
- Patch proposed changé de Non à Oui

J'ai bien vérifié que le tests passait en python2 et échouait en python3 avant de patcher shared_secret .

#3 - 05 décembre 2019 18:52 - Emmanuel Cazenave

Et comme le problème avait déjà été résolu dans hobo, on va faire pareil.

#4 - 05 décembre 2019 18:52 - Emmanuel Cazenave

- Fichier 0001-ctl-preserve-key-length-in-py3-38240.patch ajouté

Avec le patch.

#5 - 05 décembre 2019 19:16 - Frédéric Péters

Sans prêter à conséquence, celui-ci aussi pourrait être corrigé :

```
wcs/api_utils.py:         nonce = hex(random.getrandbits(128))[2:-1]
```

Et un bout dans la documentation,

```
help/fr/api-auth.page:         nonce = hex(random.getrandbits(128))[2:-1]
```

#6 - 09 décembre 2019 09:48 - Emmanuel Cazenave

- Fichier 0001-ctl-preserve-key-length-in-py3-38240.patch ajouté

Voici.

#7 - 09 décembre 2019 13:23 - Frédéric Péters

- Statut changé de Solution proposée à Solution validée

#8 - 09 décembre 2019 13:53 - Emmanuel Cazenave

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

```
commit e80f55d694b93a674076ac24d7245d686dd2da33
Author: Emmanuel Cazenave <ecazenave@entrouvert.com>
Date:   Thu Dec 5 18:43:14 2019 +0100
```

```
    ctl: preserve key length in py3 (#38240)
```

#9 - 10 décembre 2019 17:15 - Frédéric Péters

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

Fichiers

0001-ctl-preserve-key-length-in-py3-38240.patch	2,54 ko	05 décembre 2019	Emmanuel Cazenave
0001-ctl-preserve-key-length-in-py3-38240.patch	2,28 ko	05 décembre 2019	Emmanuel Cazenave
0001-ctl-preserve-key-length-in-py3-38240.patch	3,51 ko	09 décembre 2019	Emmanuel Cazenave