

Combo - Development #43563

Des tests de combo sont cassés en python3.8

03 juin 2020 10:43 - Nicolas Roche

Statut:	Fermé	Début:	03 juin 2020
Priorité:	Normal	Echéance:	
Assigné à:	Nicolas Roche	% réalisé:	0%
Catégorie:		Temps estimé:	0:00 heure
Version cible:		Planning:	Non
Patch proposed:	Oui		
Description			
<pre>\$ tox -re py3-django22 -- tests/test_utils.py ... > t = time.clock() E AttributeError: module 'time' has no attribute 'clock' /tmp/tox-nroche/combo/py3-django22/lib/python3.8/site-packages/Crypto/Random/_UserFriendlyRNG.py:7 7: AttributeError</pre>			
cf https://docs.python.org/3/whatsnew/3.8.html#api-and-feature-removals : The function time.clock() has been removed, after having been deprecated since Python 3.3: use time.perf_counter() or time.process_time() instead, depending on your requirements, to have well-defined behavior. (Contributed by Matthias Bussonnier in bpo-36895.)			
Demandes liées:			
Lié à Authentic 2 - Bug #38017: authentic2_auth_fc:Plugin ImportError('No mod...		Fermé	27 novembre 2019

Révisions associées

Révision 7494896e - 17 juin 2020 11:39 - Nicolas Roche

utils: switch to pycryptodomex, replace Crypto with Cryptodome (#43563)

Historique

#1 - 03 juin 2020 11:10 - Nicolas Roche

La librairie pycrypto ne propose pas de nouvelle version (depuis 2013) :

<https://pypi.org/project/pycrypto/#history>

<https://github.com/pycrypto/pycrypto/blob/master/ChangeLog>

Je vois qu'authentic et passerelle utilisent Cryptodome :

- `passerelle/apps/cryptor/models.py`
- `authentic/src/authentic2/crypto.py` avec du code très similaire ici.

#2 - 03 juin 2020 11:30 - Frédéric Péters

- *Sujet changé de Les tests de combo sont cassés en python3.8 à Des tests de combo sont cassés en python3.8*

#3 - 03 juin 2020 11:32 - Nicolas Roche

- *Lié à Bug #38017: authentic2_auth_fc:Plugin ImportError('No module named Crypto.Cipher,') ajouté*

#4 - 03 juin 2020 11:52 - Nicolas Roche

- *Fichier 0001-utils-use-pycryptodomex-replace-Crypto-with-Cryptodom.patch ajouté*

- *Statut changé de Nouveau à Solution proposée*

- *Patch proposed changé de Non à Oui*

Note: J'ai du modifier le code pour ne pas introduire de régression dans les tests (alors que cette modification n'est pas faite sur authentic).

```
def aes_hex_encrypt(key, data):
    iv = Random.get_random_bytes(2) * 8
    aes_key = PBKDF2(key, iv)
```

```
    aes = AES.new(aes_key, AES.MODE_CFB, iv)
-   crypted = aes.encrypt(data)
+   crypted = aes.encrypt(force_bytes(data))
    return force_text(b'%s%s' % (binascii.hexlify(iv[:2]), binascii.hexlify(crypted)))
```

#5 - 03 juin 2020 12:33 - Benjamin Dauvergne

Nicolas Roche a écrit :

Note: J'ai du modifier le code pour ne pas introduire de régression dans les tests (alors que cette modification n'est pas faite sur authentic).

Coté authentic l'API suppose qu'on ne lui passe que des bytes (je trouve ça mieux ainsi personnellement, chiffrer c'est pas niveau) :

```
    data['block']['encrypted_bindpw'] = force_text(crypto.aes_base64_encrypt(
        settings.SECRET_KEY, force_bytes(data['block']['bindpw'])))
```

#6 - 03 juin 2020 14:41 - Nicolas Roche

- Fichier 0001-utils-use-pycryptodomex-replace-Crypto-with-Cryptodom.patch ajouté

Voici une nouvelle version faisant en sorte qu'aes_hex_encrypt soit toujours appelée en lui passant des bytes.

#7 - 17 juin 2020 11:45 - Frédéric Péters

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

Validé/poussé, corrigé crypto -> crypto dans le message.

```
commit 7494896e9faa8501b24ffe3a32dc9a0d7df17a73
Author: Nicolas ROCHE <nroche@entrouvert.com>
Date: Wed Jun 3 11:27:09 2020 +0200
```

```
utils: switch to pycryptodomex, replace Crypto with Cryptodome (#43563)
```

#8 - 17 juin 2020 17:16 - Frédéric Péters

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

Fichiers

0001-utils-use-pycryptodomex-replace-Crypto-with-Cryptodom.patch	2,47 ko	03 juin 2020	Nicolas Roche
0001-utils-use-pycryptodomex-replace-Crypto-with-Cryptodom.patch	9,89 ko	03 juin 2020	Nicolas Roche