Authentic 2 - Bug #31296

authn OIDC : typo sur la signature utilisée lors de l'enregistrement d'un fournisseur distant

12 mars 2019 09:54 - Paul Marillonnet

Statut:	Fermé	**Début:**	12 mars 2019
Priorité:	Normal	**Echéance:**	
Assigné à:	Paul Marillonnet	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	

Description

Dans cette fonction register_issuer on a :

```
    elif (set(['HS256', 'HS384', 'HS512']) &
          set(openid_configuration['id_token_signing_alg_values_supported'])):
        idtoken_algo = models.OIDCProvider.HMAC
```

alors que dans les modèles la constante magique n'est pas HMAC mais ALGO_HMAC.

Révisions associées

Révision b9d98648 - 14 mars 2019 16:00 - Paul Marillonnet

oidc authn: add issuer registration testing (#31296)

Révision 89d0b7e2 - 14 mars 2019 16:00 - Paul Marillonnet

oidc authn: use correct hmac signature magic constant (#31296)

Révision 5e4e0592 - 14 mars 2019 16:00 - Paul Marillonnet

oidc authn: do not set the provider fixture's id (#31296)

Historique

#1 - 12 mars 2019 09:55 - Paul Marillonnet

(Je vais commencer par écrire un test qui fera planter cette fonction register_issuer.)

#2 - 12 mars 2019 11:11 - Benjamin Dauvergne

- Assigné à mis à Paul Marillonnet

Toujours une bonne idée d'ajouter des tests, mais je valide d'avance la correction.

#3 - 12 mars 2019 11:40 - Paul Marillonnet

- Fichier 0001-manager-unset-verified-flag-on-a-modified-email-addr.patch ajouté

- Fichier 0002-users-api-unset-verified-flag-on-a-modified-email-ad.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Assigné à Paul Marillonnet supprimé

- Patch proposed changé de Non à Oui

#4 - 12 mars 2019 11:40 - Paul Marillonnet

- Fichier 0001-manager-unset-verified-flag-on-a-modified-email-addr.patch supprimé

#5 - 12 mars 2019 11:40 - Paul Marillonnet

- Fichier 0002-users-api-unset-verified-flag-on-a-modified-email-ad.patch supprimé

#6 - 12 mars 2019 11:41 - Paul Marillonnet

- Fichier 0001-oidc-authn-add-issuer-registration-testing-31296.patch ajouté

- Fichier 0002-oidc-authn-use-correct-hmac-signature-magic-constant.patch ajouté

Pardon. Fatigue...

#7 - 12 mars 2019 12:25 - Benjamin Dauvergne

Build error.

#8 - 12 mars 2019 12:25 - Benjamin Dauvergne

- Statut changé de Solution proposée à En cours

- Assigné à mis à Paul Marillonnet

#9 - 12 mars 2019 12:40 - Paul Marillonnet

Ça ne casse que pour l'environnement virtuel dj1.8+pg :

```
================================== FAILURES ===================================
_____________________ test_register_issuer[oidc_provider2] _____________________

app = <django_webtest.DjangoTestApp object at 0x7f3d1e82f850>
caplog = <_pytest.logging.LogCaptureFixture object at 0x7f3d1f503950>
code = 'xxxx', oidc_provider = <OIDCProvider 'https://idp.example.com/'>
oidc_provider_jwkset = {'keys': _JWKkeys([<jwcrypto.jwk.JWK object at 0x7f3d1f503650>])}

    def test_register_issuer(app, caplog, code, oidc_provider, oidc_provider_jwkset):
        config_dir = os.path.dirname(__file__)
        config_file = os.path.join(config_dir, 'openid_configuration.json')
        with open(config_file) as f:
            oidc_conf = json.load(f)
        jwks_uri = urlparse.urlparse(oidc_conf['jwks_uri'])

        @urlmatch(netloc=jwks_uri.netloc, path=jwks_uri.path)
        def jwks_mock(url, request):
            return oidc_provider_jwkset.export()

        with HTTMock(jwks_mock):
            provider = register_issuer(
                    name='test_issuer',
                    issuer=oidc_provider.issuer,
>                   openid_configuration=oidc_conf)

tests/test_auth_oidc.py:460:
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
src/authentic2_auth_oidc/utils.py:277: in register_issuer
    return models.OIDCProvider.objects.create(**kwargs)
/tmp/tox-jenkins/authentic/wip/31296-typo-in-authn-oidc-utils/py27-coverage-dj18-authentic-pg-/local/lib/pytho
n2.7/site-packages/django/db/models/manager.py:127: in manager_method
    return getattr(self.get_queryset(), name)(*args, **kwargs)
/tmp/tox-jenkins/authentic/wip/31296-typo-in-authn-oidc-utils/py27-coverage-dj18-authentic-pg-/local/lib/pytho
n2.7/site-packages/django/db/models/query.py:348: in create
    obj.save(force_insert=True, using=self.db)
/tmp/tox-jenkins/authentic/wip/31296-typo-in-authn-oidc-utils/py27-coverage-dj18-authentic-pg-/local/lib/pytho
n2.7/site-packages/django/db/models/base.py:734: in save
    force_update=force_update, update_fields=update_fields)
/tmp/tox-jenkins/authentic/wip/31296-typo-in-authn-oidc-utils/py27-coverage-dj18-authentic-pg-/local/lib/pytho
n2.7/site-packages/django/db/models/base.py:762: in save_base
    updated = self._save_table(raw, cls, force_insert, force_update, using, update_fields)
/tmp/tox-jenkins/authentic/wip/31296-typo-in-authn-oidc-utils/py27-coverage-dj18-authentic-pg-/local/lib/pytho
n2.7/site-packages/django/db/models/base.py:846: in _save_table
    result = self._do_insert(cls._base_manager, using, fields, update_pk, raw)
/tmp/tox-jenkins/authentic/wip/31296-typo-in-authn-oidc-utils/py27-coverage-dj18-authentic-pg-/local/lib/pytho
n2.7/site-packages/django/db/models/base.py:885: in _do_insert
    using=using, raw=raw)
/tmp/tox-jenkins/authentic/wip/31296-typo-in-authn-oidc-utils/py27-coverage-dj18-authentic-pg-/local/lib/pytho
n2.7/site-packages/django/db/models/manager.py:127: in manager_method
    return getattr(self.get_queryset(), name)(*args, **kwargs)
/tmp/tox-jenkins/authentic/wip/31296-typo-in-authn-oidc-utils/py27-coverage-dj18-authentic-pg-/local/lib/pytho
n2.7/site-packages/django/db/models/query.py:920: in _insert
    return query.get_compiler(using=using).execute_sql(return_id)
/tmp/tox-jenkins/authentic/wip/31296-typo-in-authn-oidc-utils/py27-coverage-dj18-authentic-pg-/local/lib/pytho
n2.7/site-packages/django/db/models/sql/compiler.py:974: in execute_sql
    cursor.execute(sql, params)
```

```
/tmp/tox-jenkins/authentic/wip/31296-typo-in-authn-oidc-utils/py27-coverage-dj18-authentic-pg-/local/lib/python2.7/site-packages/django/db/backends/utils.py:64: in execute
    return self.cursor.execute(sql, params)
/tmp/tox-jenkins/authentic/wip/31296-typo-in-authn-oidc-utils/py27-coverage-dj18-authentic-pg-/local/lib/python2.7/site-packages/django/db/utils.py:98: in __exit__
    six.reraise(dj_exc_type, dj_exc_value, traceback)
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

self = <django.db.backends.utils.CursorWrapper object at 0x7f3d1f513990>
sql = 'INSERT INTO "authentic2_auth_oidc_oidcprovider" ("name", "slug", "issuer", "client_id", "client_secret", "authorizati...%s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s) RETURNING "authentic2_auth_oidc_oidcprovider"."id"'
params = ('test_issuer', None, 'https://a2test.publik/', '016fbe9d-28bd-4640-ad58-c46f57058ea8', '6f2bd534-24d6-4845-95b2-5b3cf893d595', 'https://a2test.publik/idp/oidc/authorize/', ...)

    def execute(self, sql, params=None):
        self.db.validate_no_broken_transaction()
        with self.db.wrap_database_errors:
            if params is None:
                return self.cursor.execute(sql)
            else:
>               return self.cursor.execute(sql, params)
E               IntegrityError: ERREUR:  la valeur d'une cl\xe9 dupliqu\xe9e rompt la contrainte unique \xab authentic2_auth_oidc_oidcprovider_pkey \xbb
E               DETAIL:  La cl\xe9 \xab (id)=(1) \xbb existe d\xe9j\xe0.

/tmp/tox-jenkins/authentic/wip/31296-typo-in-authn-oidc-utils/py27-coverage-dj18-authentic-pg-/local/lib/python2.7/site-packages/django/db/backends/utils.py:64: IntegrityError
```

Je creuse l'affaire.

#10 - 12 mars 2019 12:44 - Paul Marillonnet

Contrainte d'unicité sur l'attribut issuer pour un fournisseur OIDC.
Je corrige ça.
Étrange quand même que ça casse ce virtualenv seulement.

#11 - 12 mars 2019 14:49 - Paul Marillonnet

- Fichier 0001-oidc-authn-add-issuer-registration-testing-31296.patch ajouté

- Statut changé de En cours à Solution proposée

Je m'étais pris les pieds dans les fixtures, c'est corrigé ici.
Le second patch ne change pas.

#12 - 12 mars 2019 14:52 - Benjamin Dauvergne

Oui étrange surtout que cela lève une exception sur l'index de la clé primaire et pas du tout sur issuer, à mon avis ça vaut la peine de comprendre.

#13 - 12 mars 2019 14:58 - Benjamin Dauvergne

Bon là le souci c'est qu'on voit qu'on peut filer n'importe quel issuer et ça ne fait même pas de vérification que l'issuer passé correspond à l'issuer récupéré via HTTP ou passé (d'ailleurs il faudrait aussi faire un test via HTTP pour les métadonnées OIDC).

#14 - 12 mars 2019 15:06 - Paul Marillonnet

Je crois maintenant que le problème vient de la fixture oidc_provider pour laquelle on mentionne explicitement l'attribut id de l'objet créé puis retourné.
Je ne comprends pas pourquoi on fait ça (cf https://git.entrouvert.org/authentic.git/tree/tests/test_auth_oidc.py#n114).

#15 - 12 mars 2019 15:12 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> Bon là le souci c'est qu'on voit qu'on peut filer n'importe quel issuer et ça ne fait même pas de vérification que l'issuer passé correspond à l'issuer récupéré via HTTP ou passé (d'ailleurs il faudrait aussi faire un test via HTTP pour les métadonnées OIDC).

C'est, je crois, un autre problème encore. #31318.

#16 - 12 mars 2019 15:23 - Paul Marillonnet

- Fichier 0001-oidc-authn-add-issuer-registration-testing-31296.patch ajouté

Et bien sûr les tests tapent maintenant dans la base, il faut rajouter un marks.db.
Je l'ai mis au début du fichier de tests, comme c'est le cas pour beaucoup d'autres.

#17 - 12 mars 2019 15:45 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> Je crois maintenant que le problème vient de la fixture oidc_provider pour laquelle on mentionne explicitement l'attribut id de l'objet créé puis retourné.
> Je ne comprends pas pourquoi on fait ça (cf https://git.entrouvert.org/authentic.git/tree/tests/test_auth_oidc.py#n114).

Effectivement c'est con, tu peux défaire, et je ne sais pas pourquoi j'ai fait ça.

#18 - 12 mars 2019 16:10 - Paul Marillonnet

- Fichier 0001-oidc-authn-add-issuer-registration-testing-31296.patch ajouté

- Fichier 0002-oidc-authn-use-correct-hmac-signature-magic-constant.patch ajouté

- Fichier 0003-oidc-authn-do-not-set-the-provider-fixture-s-id-3129.patch ajouté

Benjamin Dauvergne a écrit :

> Effectivement c'est con, tu peux défaire, et je ne sais pas pourquoi j'ai fait ça.

Je préfère faire ça dans un commit à part.

#19 - 12 mars 2019 16:54 - Benjamin Dauvergne

C'est perso mais je n'aime pas pytestmark = pytest.mark.django_db je préfère un db dans la signature du test, "explicit is better than implicit".

Test foirant sur un test n'ayant aucun rapport j'ai relancé.

#20 - 12 mars 2019 19:26 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

Ack, mais je veux bien que tu enlèves pytest.mark.

#21 - 14 mars 2019 13:22 - Benjamin Dauvergne

Go.

#22 - 14 mars 2019 16:02 - Paul Marillonnet

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

```
commit 5e4e0592ec67bd9ec42dbf8df7aa85f87cc03746
Author: Paul Marillonnet <pmarillonnet@entrouvert.com>
Date:   Tue Mar 12 16:06:28 2019 +0100

    oidc authn: do not set the provider fixture's id (#31296)

commit 89d0b7e2da9386807de443bc122419f8b5e89000
Author: Paul Marillonnet <pmarillonnet@entrouvert.com>
Date:   Tue Mar 12 11:38:55 2019 +0100

    oidc authn: use correct hmac signature magic constant (#31296)

commit b9d98648d2254cf27732be18965f4e17aa8c0c99
Author: Paul Marillonnet <pmarillonnet@entrouvert.com>
Date:   Tue Mar 12 11:38:12 2019 +0100

    oidc authn: add issuer registration testing (#31296)
```

#23 - 19 mars 2019 12:15 - Frédéric Péters

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

Fichiers

0001-oidc-authn-add-issuer-registration-testing-31296.patch	2,38 ko	12 mars 2019	Paul Marillonnet

0002-oidc-authn-use-correct-hmac-signature-magic-constant.patch	1,09 ko	12 mars 2019	Paul Marillonnet
0001-oidc-authn-add-issuer-registration-testing-31296.patch	2,37 ko	12 mars 2019	Paul Marillonnet
0001-oidc-authn-add-issuer-registration-testing-31296.patch	2,55 ko	12 mars 2019	Paul Marillonnet
0001-oidc-authn-add-issuer-registration-testing-31296.patch	2,56 ko	12 mars 2019	Paul Marillonnet
0002-oidc-authn-use-correct-hmac-signature-magic-constant.patch	1,09 ko	12 mars 2019	Paul Marillonnet
0003-oidc-authn-do-not-set-the-provider-fixture-s-id-3129.patch	742 octets	12 mars 2019	Paul Marillonnet