Hobo - Bug #41423

gestion du nonce dans la signature : verifier seulement s'il existe

07 avril 2020 14:18 - Thomas Noël

Statut:	En cours	**Début:**	07 avril 2020
Priorité:	Normal	**Echéance:**	
Assigné à:	Thomas Noël	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Dans le code de vérification de signature, j'ai récemment fait ceci :

```
    if known_nonce is not None:
        if ('nonce' not in parsed) or known_nonce(parsed['nonce'][0]):
            return False
```

C'est à dire que si une fonction de vérification du nonce existe, elle rend le nonce obligatoire.

Je pense que c'est une mauvaise idée, il faut plutôt faire comme dans wcs : vérifier le nonce s'il existe, et sinon laisser filer.

L'idée étant que le nonce est une protection que se donne l'appelant contre le rejeu, mais l'appelé ça ne le concerne pas.

Historique

#1 - 07 avril 2020 14:21 - Thomas Noël

- Assigné à mis à Thomas Noël

#2 - 07 avril 2020 14:23 - Frédéric Péters

Ce serait pas mieux de plutôt le gérer ? De manière sommaire via le cache django, c'est pas sûr 100% mais ça coûte rien.

#3 - 07 avril 2020 14:38 - Thomas Noël

- Fichier 0001-signature-verify-nonce-only-if-it-exists-41362.patch ajouté

- Statut changé de Nouveau à En cours

- Patch proposed changé de Non à Oui

Frédéric Péters a écrit :

> Ce serait pas mieux de plutôt le gérer ? De manière sommaire via le cache django, c'est pas sûr 100% mais ça coûte rien.

Ah oui j'avais pas pensé à ça. Bon, entre temps j'ai quand même patché l'idée de ce ticket, mais y'a pas d'urgence, je prendrais le temps de compléter ce patch avec un vrai "known_nonce". (je ne mets donc pas de "solution proposée" encore)

Ceci dit si l'attaquant sait que les nonce sont cachés par node, il lui suffira de renvoyer l'attaque sur les deux nodes. Il a une technique d'attaque qui devient "sûre à 100%"...?

#4 - 07 avril 2020 14:47 - Frédéric Péters

Oui à 100% on passe de nonce à ntwice.

Fichiers

0001-signature-verify-nonce-only-if-it-exists-41362.patch	2,19 ko	07 avril 2020	Thomas Noël