Passerelle - Development #43122

cryptor : utiliser un hachage plus fort

20 mai 2020 02:27 - Thomas Noël

Statut:	Fermé	**Début:**	20 mai 2020
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

L'algorithme de hachage SHA1 est utilisé par l'algorithme de chiffrement de la clé secrète RSA-OAEP servant à protéger les fichiers au repos.

Il est recommandé de remplacer l'algorithme utilisé avec OEAP par SHA512/256.

Révisions associées

Révision 9dab5b70 - 21 mai 2020 15:36 - Thomas Noël

cryptor: use sha512 for OAEP hash function (#43122)

Historique

#2 - 21 mai 2020 00:12 - Thomas Noël

- Fichier 0001-cryptor-use-sha512-for-OAEP-hash-function-43122.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#3 - 21 mai 2020 10:53 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

Zyva SHA512 direct. Ok.

#4 - 21 mai 2020 15:36 - Thomas Noël

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

```
commit 9dab5b70e7e87f001dafc93533672d095663aa59
Author: Thomas NOEL <tnoel@entrouvert.com>
Date:   Thu May 21 00:11:49 2020 +0200

    cryptor: use sha512 for OAEP hash function (#43122)
```

#5 - 22 mai 2020 11:16 - Frédéric Péters

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

Fichiers

0001-cryptor-use-sha512-for-OAEP-hash-function-43122.patch	1,71 ko	20 mai 2020	Thomas Noël