Distribution EOLE - Demande #17458

Outrepasser la désactivation par défaut des clef DSA dans la configuration OpenSSH

12/10/2016 12:09 - samuel morin

Statut:	Fermé	**Début:**	12/10/2016
Priorité:	Normal	**Echéance:**	
Assigné à:	Luc Bourdot	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:		**Temps passé:**	0.00 heure

Description

avec les dernières version d'openssh, les connexions par clé dsa ont été désactivées.
serait-il possible de prévoir de les réactiver, sachant que l'algo dsa ne semble pas poser de problème en terme de sécurité ?
PubkeyAcceptedKeyTypes=+ssh-dss

Historique

#1 - 13/10/2016 09:20 - Daniel Dehennin

- Sujet changé de Eole 2.6 ajout paramètre dans sshd_config à Outrepasser la désactivation par défaut des clef DSA dans la configuration OpenSSH

- Assigné à mis à Luc Bourdot

D'après la documentation d'OpenSSH:

> OpenSSH 7.0 and greater similarly disable the ssh-dss (DSA) public key algorithm. It too is weak and we recommend against its use.

Il faudra donc voir avec le product owner pour une décision du pôle.

Pour ma part je propose de le gérer comme #15846#note-2

#2 - 07/11/2016 14:37 - Daniel Dehennin

C'est aussi la recommandation №7 du document de l'ANSSI de désactiver DSA, du fait d'une taille de clef limitée, comme très bien expliquée sur security.stackexchange.

#3 - 22/11/2016 11:14 - Luc Bourdot

Ok avec la proposition de Daniel de le gérer comme #15846

#4 - 01/12/2016 10:55 - Gérald Schwartzmann

Bonjour la demande #15846 est fermée,

La demande est-elle toujours d'actualité ?

Merci d'avance

#5 - 06/12/2016 11:11 - Luc Bourdot

- Statut changé de Nouveau à Fermé