# Contrôleurs de domaine prennent en charge les types de chiffrement RC4 ou DES

ID METSYS : 25  
ID PurplKnight : [RC4 or DES encryption type are supported by Domain Controllers](https://www.purple-knight.com/fr/security-indicators/)

Charge de travail : 1 jour  
Difficulté : 2 - Requière quelques connaissances sur l'infrastructure et l'anomalie qu'elle contient

****Description****

Le RC4 et le DES sont considérés comme des formes de chiffrement non sécurisées, susceptibles à diverses attaques cryptographiques. De multiples vulnérabilités dans les algorithmes RC4 et DES permettent des attaques de type « MitM » et de déchiffrement. Voir les « CVE-2013-2566 » et « CVE-2015-2808 ».

****Recommandation****

Il est recommandé de désactiver la prise en charge de RC4 et DES sur les contrôleurs de domaine. Procédez avec prudence, car cela peut entraîner des échecs pour les clients qui demandent par défaut des tickets Kerberos chiffrés en RC4.

Désactivez-les en ajoutant la stratégie de groupe « Configuration de la sécurité réseau : Configuration des types de chiffrement autorisés pour Kerberos » et sélectionnez uniquement les types de chiffrement « AES-128 » et « AES-256 », dans une GPO qui affecte le conteneur des contrôleurs de domaine. Le chemin de la stratégie de groupe est « Configuration de l'ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Options de sécurité ».