# Utilisation de mots de passe réversibles pour les comptes d'utilisateurs

ID METSYS : 42  
ID PingCastle : [S-Reversible](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)  
ID PurplKnight : [User accounts that store passwords with reversible encryption](https://www.purple-knight.com/fr/security-indicators/)  
ID ANSSI : [vuln3\_reversible\_password](https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#reversible_password)

Charge de travail : 0.5 jour  
Difficulté : 1 - Requière quelques connaissances sur l'anomalie

****Description****

Il est possible que des domaines aient des comptes avec un chiffrement réversible. Dans ce cas, cela signifie que le mot de passe est réellement stocké en texte clair dans l'attribut « supplementalCredential » du compte et qu'il peut être récupéré à l'aide d'une attaque « DCSync ».

****Recommandation****

Pour éliminer ce risque, il ne devrait y avoir aucun compte avec un chiffrement réversible. Vous devez les supprimer en supprimant le drapeau « Stocker le mot de passe en utilisant un chiffrement réversible » sur tous les comptes, de sorte que le mot de passe en texte clair soit supprimé lors du prochain changement de mot de passe.

Vous pouvez obtenir une liste de tous les comptes potentiellement compromis en exécutant la commande PowerShell suivante :

Get-adobject -ldapfilter "(userAccountControl:1.2.840.113556.1.4.803:=128)" -properties useraccountcontrol