# Attributs « unixUserPassword » et « userPassword »

ID METSYS : 52  
ID PingCastle : [A-UnixPwd](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)  
ID ANSSI : [vuln3\_reversible\_password](https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#reversible_password)

Charge de travail : 1 jour  
Difficulté : 3 - Requière des connaissances avancées sur l'anomalie

****Description****

Pour effectuer une authentification unique (SSO), les systèmes doivent partager des secrets avec Active Directory. Ce n'est pas le cas pour tous les systèmes tels que Unix et Mainframe, et les concepteurs ont trouvé une solution de contournement en stockant ce secret dans un attribut du compte utilisateur. Cependant, tous les systèmes n'ont pas mis en œuvre un protocole approprié et cryptographiquement sûr, et ils vérifient le mot de passe soumis dans leur système avec un attribut AD.

À l'époque, on ne savait pas que ces attributs pouvaient être interrogés par n'importe qui, et par conséquent, aucune protection robuste n'a été mise en place. En examinant l'attribut « unixUserPassword », le mot de passe peut être récupéré soit en texte clair (encodé en ASCII) soit avec un algorithme faible tel que ROT 13.

De plus, la manière de changer un mot de passe dans un système LDAP est de modifier la valeur de l'attribut spécial « userPassword ». Cet attribut n'est pas censé être visible. Cependant, Active Directory utilise un autre attribut nommé « unicodePwd » (sauf si l'heuristique « fUserPwdSupport » est activée). Cela signifie que l'attribut « userPassword » n'est plus spécial et qu'un changement de sa valeur est affiché en texte clair, considéré comme un attribut normal. Une application mal configurée peut changer le mot de passe de l'utilisateur en utilisant ce vieux mécanisme et, par conséquent, définir le mot de passe de l'utilisateur en texte clair.

****Recommandation****

Les attributs « unixUserPassword » et « userPassword » des comptes utilisateur mentionnés doivent être effacés, sauf si le système distant est connu pour avoir un protocole cryptographique solide.