# Mots-de-passe LAPS pouvant être récupérés à partir des ordinateurs ajoutés manuellement par les utilisateurs

ID METSYS : 35  
ID PingCastle : [A-LAPS-Joined-Computers](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html), [S-ADRegistration](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)  
ID PurplKnight : [Changes to MS LAPS read permissions](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****

Par défaut, chaque utilisateur du domaine peut ajouter jusqu'à 10 ordinateurs au domaine. Lorsqu'un ordinateur est ajouté au domaine, le propriétaire de l'objet d'ordinateur est l'utilisateur qui a ajouté l'ordinateur. Pour tracer cette insertion, un attribut spécial « mS-DS-CreatorSID » est ajouté, dont la valeur est le SID de son créateur.

Lorsque LAPS est installé, le compte administrateur local a son mot de passe stocké dans un attribut spécial nommé, par défaut, « ms-mcs-AdmPwd ». Son accès est restreint. Étant donné que l'utilisateur qui l'a créé est le propriétaire de l'objet sous-jacent, il peut récupérer l'attribut LAPS et obtenir le mot de passe de l'administrateur local.

Le droit « tous les droits étendus » permet de lire le mot de passe LAPS et l'accès en écriture à ces attributs peut annuler le renforcement de la sécurité en modifiant le propriétaire.

****Recommandation****

Examiner la sécurité des objets d'ordinateur répertoriés dans la section LAPS ci-dessous pour changer leur propriétaire (vous pouvez le donner au groupe des administrateurs de domaine). Vérifier si le créateur a également des autorisations d'écriture pour changer le propriétaire ou le descripteur de sécurité et s'il dispose du droit « tous les droits étendus » sur cet objet. Si c'est le cas, supprimer les autorisations accordées à cet utilisateur.