# Domaines utilisés dans l’historique SID

ID METSYS : 2  
ID PingCastle : [*T-SIDHistoryUnknownDomain*](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html), [*S-SIDHistory*](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)  
ID ANSSI : [*vuln3\_sidhistory\_present*](https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#sidhistory_present)

Charge de travail : 5 jours  
Difficulté : 1 - Requière quelques connaissances sur l'anomalie

****Description****

La présence de SIDHistory dans le domaine peut être exploitée (difficilement) pour des attaques. En principe la présence de SIDHistory devrait être temporaire seulement pendant la phase de migration puis un nettoyage exhaustif devrait être réalisé.

****Recommandation****

Chaque descripteur de sécurité du domaine (y compris les partages de fichiers par exemple) doit être examiné et réécrit avec le nouveau SID du compte. Ensuite, l'attribut « SID History » doit être supprimé.

Pour supprimer tous les attributs « SIDHistory ». Pour ce faire, vous pouvez répertorier les objets ayant cet attribut à l'aide de la commande suivante :

get-ADObject -ldapfilter "(sidhistory=\*)" -properties sidhistory

Chaque descripteur de sécurité du domaine, y compris les partages de fichiers par exemple, doit être examiné pour être réécrit avec le nouveau SID du compte. Ensuite, l'attribut peut être supprimé de ces comptes à l'aide de l'outil de migration ou d'un extrait de code PowerShell « Remove-SIDHistory » une fois la migration terminée.

Veuillez noter qu'une fois que le « SIDHistory » a été supprimé, il ne peut pas être rétabli sans effectuer une véritable migration. Des outils de piratage tels que « Mimikatz » pourraient être utilisés pour annuler une suppression, par exemple avec l'attaque « lsadump::dcshadow ».

Pour supprimer le « SIDHistory » d'un compte utilisateur, exécutez :

Get-ADUser NOM\_UTILISATEUR -properties sidhistory | foreach {Set-ADUser $\_ -remove @{sidhistory=$.sidhistory.value}}

Pour un groupe, exécutez :

Get-ADGroup NOM\_GROUPE -properties sidhistory | foreach {Set-ADGroup $ -remove @{sidhistory=$.sidhistory.value}}

Pour tous les utilisateurs d'une unité d'organisation (OU) :

Get-ADUser -SearchBase "OU=Comptes,DC=mondomaine,DC=com" -Filter {sidhistory -like '\*'} -properties sidhistory | foreach {Set-ADUser $ -remove @{sidhistory=$\_.sidhistory.value}}