# Contexte

Si l’historique d’identificateurs de sécurité est utilisé lors d’une migration, alors celui-ci doit être supprimé au plus vite après la fin de la migration.

Lorsque le filtrage d’identificateurs de sécurité est désactivé, autrement dit, lorsque l’historique d’identificateurs de sécurité n’est pas utilisé, mais qu’un historique d’identificateurs de sécurité est tout de même présenté lors d’une requête d’accès aux ressources du domaine venant d’une relation de confiance, alors plusieurs scénarios sont possibles en fonction de la configuration du contrôle d’authentification Active Directory :

* Acceptation de l’authentification sans tenir compte de l’historique d’identificateurs de sécurité.
* Rejet de l’authentification.
* Rejet de l’authentification et mise en quarantaine de la relation de confiance.

# Conséquences

Désactiver l’historique d’identificateurs de sécurité permet d’éviter les scénarios suivants :

* **Déplacement latéral** : Si un attaquant obtient l'accès à un compte utilisateur avec l'historique d’identificateurs de sécurité activé, il pourrait exploiter cette fonctionnalité pour se déplacer latéralement dans le réseau. En se faisant passer pour un utilisateur d'un autre domaine ou d'une autre forêt avec des privilèges élevés, l'attaquant pourrait accéder à des ressources dans d'autres domaines ou forêts où l'utilisateur compromis a des autorisations.
* **Élévation de privilèges** : Si un attaquant compromet un compte utilisateur avec l'historique d’identificateurs de sécurité activé et parvient à élever ses privilèges dans son propre domaine, il pourrait exploiter l'historique d’identificateurs de sécurité pour escalader davantage les privilèges dans d'autres domaines ou forêts où l'utilisateur compromis a des autorisations historiques. Cela pourrait conduire à l'obtention d'un accès administratif à des systèmes critiques ou à des données sensibles.
* **Persistance** : Un attaquant qui obtient l'accès à un environnement peut tenter d'établir une présence persistante en modifiant l'historique d’identificateurs de sécurité des comptes utilisateur compromis. En ajoutant leur propre identificateur de sécurité à l'historique d'un compte à privilèges élevés, l'attaquant pourrait maintenir l'accès aux ressources même si leur accès initial est détecté et corrigé.

## Chaine de cyberattaques

Désactivé l’historique d’identificateurs de sécurité permet d’éviter l’accomplissement des étapes suivantes d’une chaine de cyberattaques :

* **Reconnaissance** : La désactivation de l'historique d’identificateurs de sécurité rend plus difficile pour les attaquants de tirer parti des autorisations historiques lors des activités de reconnaissance.
* **Exploitation** : La désactivation de l'historique d’identificateurs de sécurité peut rendre plus difficile pour les attaquants d'exploiter les relations de confiance entre les domaines ou les forêts, limitant leur capacité à escalader les privilèges et à se déplacer latéralement dans le réseau.
* **Installation** : La désactivation de l'historique d’identificateurs de sécurité peut aider à empêcher les attaquants d'utiliser des identifiants compromis avec des autorisations historiques pour maintenir la persistance dans l'environnement.
* **Commande et contrôle** : La désactivation de l'historique d’identificateurs de sécurité peut perturber la capacité des attaquants à se faire passer pour des utilisateurs avec des autorisations historiques, rendant plus difficile pour eux d'éviter la détection et de contrôler les systèmes compromis.

# Détection

Les commandes PowerShell suivantes permettent de connaître l’état des fonctionnalités d’historique d’identificateurs de sécurité (SID History) et de filtrage des identificateurs de sécurité (SID Filtering) des relations de confiance (Trust) avec le domaine courant :

#

# Installer le module PowerShell Active Directory

#

#Install-Module ActiveDirectory

#

# Importer le module PowerShell Active Directory

#

Import-Module ActiveDirectory

#

# Vérifier l'état du filtrage des identificateurs de sécurité dans les relations de confiance entre deux domaines

#

# Documentation : https://learn.microsoft.com/en-us/powershell/module/activedirectory/get-adtrust?view=windowsserver2022-ps

# -filter \* : Sélectionner toutes les relations de confiance

# select name,target,sid\* : Pour chaque relation de confiance, sélectionner :  
# - name : Le nom de la relation de confiance  
# - target : Le domaine de confiance  
# - SIDFilteringForestAware : L’état de la fonctionnalité d’historique d’identificateurs de sécurité (SID History)  
# - SIDFilteringQuarantined : L’état de la fonctionnalité de quarantaine  
#

get-adtrust -filter \* | select name,target,sid\*

Pour chaque relation de confiance, l’historique d’identificateurs de sécurité devrait être désactivé (False) et la fonctionnalité de quarantaine devrait être active (True).

Documentation :

* <https://learn.microsoft.com/en-us/powershell/module/activedirectory/get-adtrust?view=windowsserver2022-ps>

# Correction

## Prérequis

Afin de corriger l’anomalie, il faut d’abord s’assurer que les relations de confiance ne sont pas entre domaines d’une même forêt. Car le filtrage des identificateurs de sécurité dans une relation de confiance entre domaines d’une même forêt n’est pas une configuration supportée et peut provoquer des erreurs. Si un domaine au sein d’une forêt n’est pas digne de confiance, alors il faut d’abord séparer les domaines de confiance et les autres domaines dans des forêts différentes. Ainsi, le filtrage des identificateurs de sécurité pourra être appliqué entre les forêts.

Ensuite, il faut s’assurer qu’aucune migration de domaine légitime ne soit en cours, car l’activation du filtrage des identificateurs de sécurité sur un domaine qui est en cours de migration pourrait compromettre le bon fonctionnement des comptes dont l’ancien identificateur de sécurité est encore utilisé dans des listes de contrôle d’accès (ACL) sur le nouveau domaine. Si une migration est en cours, celle-ci doit être terminée au plus vite et les anciens identificateurs de sécurité ne doivent plus être utilisés.

Pour pouvoir exécuter les commandes suivantes, l’utilisateur doit faire partie du groupe d’administrateurs du domaine, *domain administrators* en anglais, ou d’administrateurs de l’entreprise, *enterprise administrators* en anglais, et le système d’exploitation doit faire partie de la liste suivante :

* Windows 8
* Windows Server 2008
* Windows Server 2008 R2
* Windows Server 2012

Documentation :

* <https://attack.mitre.org/techniques/T1134/005/>
* <https://learn.microsoft.com/fr-fr/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc835085(v=ws.11)>

## Procédure

Pour commencer, il est recommandé de supprimer les historiques d’identificateurs de sécurité des comptes et groupes d’utilisateurs du domaine.

Les commandes PowerShell suivantes permettent de supprimer l’historique d’identificateurs de sécurité de tous les utilisateurs et groupes d’utilisateurs du domaine :

#

# Installer le module Active Directory  
#

# Install-Module ActiveDirectory

#

# Importer le module Active Directory

#

Import-Module ActiveDirectory

#

# Rechercher tous les utilisateurs du domaine

#

$Users = Get-ADObject -Filter {ObjectClass -eq "user"} -Properties sidHistory  
  
#  
# Rechercher tous les groupes d’utilisateurs du domaine  
#

$Groups = Get-ADObject -Filter {ObjectClass -eq "group"} -Properties sidHistory

#

# Pour chaque utilisateur

#

foreach ($User in $Users) {

#

# Si l’utilisateur a un historique d’identificateurs de sécurité

#

if ($User.sidHistory) {  
 #  
 # Supprimer l’historique d’identificateurs de sécurité

#

$User.sidHistory = $null

#

# Appliquer la modification

#

Set-ADObject -Instance $User  
 }

}

#

# Pour chaque groupe d’utilisateurs

#

foreach ($Group in $Groups) {

#

# Si le groupe d’utilisateurs a un historique d’identificateurs de sécurité

#

if ($Group.sidHistory) {

#  
 # Supprimer l’historique d’identificateurs de sécurité

#

$Group.sidHistory = $null

#

# Appliquer la modification

#

Set-ADObject -Instance $Group

}

}

Ensuite, il est recommandé de désactiver l’utilisation de l’historique d’identificateurs de sécurité (SID History) pour les relations de confiance (Trust) entre forêts.

Les commandes Netdom suivantes permettent de désactiver l’utilisation de l’historique d’identificateurs de sécurité sur un domaine Active Directory :

#

# Désactiver l’historique d’identificateurs de sécurité sur un domaine Active Directory :

# - Le domaine ne transmettra plus l’historique d’identificateurs de sécurité lors de l’envoi de requêtes vers un autre domaine.  
# - Le domaine ne s’attendra plus à recevoir l’historique d’identificateurs de sécurité lors de la réception de requêtes depuis un autre domaine.

#

netdom trust <domaine confiant> /domain:<domaine de confiance> /EnableSIDHistory:no

Les commandes Netdom suivantes permettent d’activer la fonctionnalité de mise en quarantaine des relations de confiance externes dans le cadre du filtrage des identificateurs de sécurité (SID Filtering) :

#

# Activer la fonctionnalité de mise en quarantaine des relations de confiance externes dans le cadre du filtrage des identificateurs de sécurité (SID Filtering) :  
# - Lorsque le domaine confiant reçoit une requête d’accès aux données du domaine contenant un historique d’identificateurs de sécurité (SID History), alors la requête sera rejetée et la relation de confiance (Trust) avec le domaine de confiance sera mise en quarantaine

#

netdom trust <domaine confiant> /domain:<domaine de confiance> /quarantine:yes

Documentation :

* <https://learn.microsoft.com/fr-fr/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc835085(v=ws.11)>

# Vérification

Pour vérifier la bonne correction de l’anomalie, il est possible de d’exécuter à nouveau la partie "Détection" et de constater que pour chaque relation de confiance entre forêts, l’historique d’identificateurs de sécurité est désactivé (False) et la fonctionnalité de quarantaine est active (True).