# Contexte

L’algorithme de chiffrement DES peut être utilisé par Kerberos lors de l’authentification d’un compte utilisateur du domaine. Cependant cet algorithme est aujourd’hui trop faible pour être utilisé lors de la création de tickets Kerberos, car il serait possible de craquer facilement ces tickets afin d’y récupérer le jeton de l’utilisateur et ainsi de compromettre le compte utilisateur du domaine.

# Conséquences

L’utilisation de l’algorithme de chiffrement DES peut avoir des impacts significatifs :

* **Élévation de privilèges** : Utiliser un algorithme de chiffrement Kerberos faible peut permettre aux attaquants d’obtenir un accès non autorisé à un compte utilisateur.
* **Persistance** Utiliser un algorithme de chiffrement Kerberos faible peut permettre aux attaquants d’obtenir l’accès à plusieurs comptes afin d’assurer une persistance sur le système.

## Chaine de cyberattaques

L’utilisation de l’algorithme de chiffrement DES peut permettre l’accomplissement des étapes suivantes d’une chaine de cyberattaques :

* **Exploitation** : La compromission de tickets Kerberos illégitimes peut permettre de donner un accès à des services présentant une faille de sécurité et ainsi permettre d’exploiter des vulnérabilités.
* **Installation** : La compromission de tickets Kerberos peut permettre la création d’accès permanent au systèmes compromis en offrant des droits administrateurs sur les systèmes de sécurité.
* **Commande** **et** **contrôle** : La compromission de tickets Kerberos illégitimes peut permettre le contrôle d’exécutables.
* **Actions** **sur** **objectif** : La compromission de tickets Kerberos illégitimes peut permettre la lecture ou l’écriture de données sur l’ensemble des systèmes compromis, rendant possible, par exemple, le vol de données.

# Détection

Les commandes PowerShell ci-dessous permettent de lister les utilisateurs du domaine utilisant l’algorithme de chiffrement DES :

#

# Importe le module PowerShell Active Directory

#

Import-Module ActiveDirectory

#

# Récupère les utilisateurs du domaine pour lesquels le chiffrement DES est actif

#

$usersWithDES = Get-ADUser -Filter {UserAccountControl -band 0x200000} -Properties SamAccountName, UserAccountControl

#

# Affiche les résultats dans la console  
#

Write-Host $usersWithDES | ForEach-Object { Write-Host $\_.SamAccountName }

Les commandes PowerShell ci-dessus ne doivent retourner aucun résultat.

# Correction

## Procédure

Les commandes PowerShell suivantes permettent de désactiver l’algorithme de chiffrement DES pour tous les comptes utilisateurs du domaine pour lesquels celui-ci est actif :

#

# Importe le module PowerShell Active Directory

#

Import-Module ActiveDirectory

#

# Récupère les utilisateurs du domaine pour lesquels le chiffrement DES est actif

#

$usersWithDES = Get-ADUser -Filter {UserAccountControl -band 0x200000} -Properties SamAccountName, UserAccountControl

#  
# Si des utilisateurs utilisent l’algorithme DES  
#

if ($usersWithDES.Count -gt 0) {  
 #

# Pour chaque utilisateur qui utilise l’algorithme DES  
 #  
 foreach ($user in $usersWithDES) {  
 #  
 # Retirer le bit correspondant à l'algorithme DES  
 #

$newUAC = $user.UserAccountControl -band (-bnot 0x200000)

#  
 # Mettre à jour les propriétés de l'utilisateur  
 #

Set-ADUser -Identity $user.SamAccountName -UserAccountControl $newUAC

#  
 # Afficher l’utilisateur mis-à-jour dans la console  
 #

Write-Host $user.SamAccountName

}

Les commandes PowerShell ci-dessus doivent afficher tous les utilisateurs pour lesquels l’utilisation de l’algorithme de chiffrement DES a été désactivé.

# Vérification

Pour vérifier la bonne correction de l’anomalie, il est possible d’exécuter à nouveau la partie "Détection" et de constater qu’aucun compte utilisateur n’est listé.