# Contexte

Le service d’impression, *print spooler* en anglais, par défaut de Windows est un service rendu par le système d’exploitation. Il gère les tâches d’impression, notamment la file d’attente ou l’ordonnancement.

Le service d’impression Windows est activé par défaut sur les contrôleurs de domaines. Cependant, plusieurs failles de sécurité critiques ont été découvertes au sein de ce service. Par exemple, la liste de failles *PrintNightmare* permet l’exécution de code à distance avec des privilèges élevés.

Un service d’impression n’est généralement pas utile sur un contrôleur de domaine, c’est pourquoi il est conseillé de le désactiver.

# Conséquences

La correction de cette anomalie permet d’éviter les scénarios suivants :

* **Élévation de Privilèges** : Un attaquant ayant accès limité peut utiliser ces vulnérabilités pour obtenir des privilèges administratifs sur le contrôleur de domaine, compromettant l'ensemble de l'infrastructure Active Directory.

## Chaine de cyberattaques

La correction de cette anomalie permet d’éviter l’accomplissement des étapes suivantes de la chaine de cyberattaque :

* **Exploitation** : La vulnérabilité du service d'impression sur le contrôleur de domaine est exploitée pour exécuter du code arbitraire à distance ou élever les privilèges.

# Détection

Les commandes PowerShell suivantes permettent de connaître l’état du service d’impression Windows :

#

# Récupère le service

#

$spoolerService = Get-Service -Name Spooler

#

# Affiche l'état du service dans la console

#

Write-Output "Status: $($spoolerService.Status)"

#

# Récupère le mode de démarrage du service

#

$spoolerStartupType = Get-WmiObject -Query "SELECT StartMode FROM Win32\_Service WHERE Name='Spooler'"

#

# Affiche le mode de démarrage du service dans la console   
#

Write-Output "StartMode: $($spoolerStartupType.StartMode)"

Le statut du service doit être "Stopped" et son mode de démarrage doit être "Disabled"

# Correction

## Procédure

Les commandes PowerShell suivantes permettent de d’arrêter le service d’impression Windows et de désactiver son démarrage automatique au démarrage du système :

#

# Arrête le service d’impression

#

Stop-Service -Name Spooler -Force

#  
# Désactive le démarrage automatique du service au démarrage du système  
#

Set-Service -Name Spooler -StartupType Disabled

# Vérification

Pour vérifier la bonne correction de l’anomalie, il est possible de d’exécuter à nouveau la partie "Détection" et de constater que le statut du service est "Stopped" et son mode de démarrage est "Disabled".