# Contexte

Les attaquants peuvent exploiter une faille dans « AD CS Web Enrollment » qui permet les attaques de relais NTLM pour s'authentifier en tant qu'utilisateur privilégié.

Une attaque par relais NTLM tire parti de la conception du protocole NTLM. Le protocole NTLM ne comporte pas d'authentification mutuelle et est donc susceptible de faire l'objet d'attaques de type "man-in-the-middle", y compris d'une attaque par relais NTLM.

Dans ce type d'attaque, un acteur de la menace capture une session d'authentification NTLM. L'attaquant relaie ensuite les informations d'identification capturées pour s'authentifier auprès d'autres services, s'appuyant ainsi sur l'identité de l'utilisateur.

Vous êtes potentiellement vulnérable à cette attaque si vous utilisez les services de certificats Active Directory (AD CS) avec l'un des services suivants :

* Inscription Web de l'autorité de certification (CA)
* Service web d'inscription de certificats (CES)

# Conséquences

La présence de la faille permettant les attaques relais NTLM peut participer à l’introduction des risques suivants :

* **Usurpation d’identité :** Un attaquant récupérant une session d’authentification NTLM peut mener des actions en se faisant passer pour l’utilisateur correspondant.
* **Élévation de privilèges :** Si un attaquant cible, à travers une attaque relais NTLM, un compte à haut privilèges, celui-ci pourrait prendre le contrôle d’une session d’authentification. Il pourra alors mener des actions nécessitant des privilèges, comme s’octroyer des privilèges.

## Chaine de cyberattaques

La présence de la faille permettant les attaques relais NTLM peut participer à l’accomplissement des étapes suivantes d’une chaine de cyberattaques :

* **Exploitation :** La vulnérabilité présente la possibilité pour un attaquant d’exploiter des outils malveillants mis en place auparavant nécessitant des privilèges obtenus par la compromission d’une session à privilège.
* **Installation :** L’utilisation d’un relais NTLM permettrai à un attaquant d’utiliser la vulnérabilité afin d’accéder à une session ayant des privilèges afin d’y installer des codes malveillants.

# Détection

Afin de détecter si le renouvellement de certificats via http est activé, il faut vérifier la présence de plusieurs interfaces :

* L’application d’inscription des certificats via l’interface web à l’adresse *http://<ADCS>/certsrv*
* Le service d’inscription des certificats (CES) accessible via l’adresse *https://<ADCS>/<NOM CA>\_CES\_Kerberos/service.svc*
* Le service d'inscription d'appareil réseau (NDES) disponible via   
  *https://<ADCS>/CertSrv/mscep*

Via la surveillance du trafic réseau, NTLM et ARP, il est possible de détecter une attaque par relais NTLM mais cela reste plus complexe.

Documentation :

* <https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/certificate-authority-web-enrollment>
* <https://learn.microsoft.com/en-us/windows-server/identity/solution-guides/certificate-enrollment-certificate-key-based-renewal>
* <https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/network-device-enrollment-service-overview>

# Correction

En premier temps, si l’inscription de certificats via un interface web n’as pas d’utilité identifié connue, il est préférable de la désactiver.

Par la suite, si l’inscription des certificats est permise via http (et non https), il est important de désactiver cet accès non sécurisé en forçant l’utilisation du protocole SSL.

De plus, si l’authentification via NTLM est activée sur le serveur AD CS, il est impératif d’activer la protection étendue pour l’authentification (EPA). Si possible, il est aussi recommandé de désactiver l’authentification NTLM sur les contrôleurs de domaines, les serveurs AD CS et pour la console IIS (Internet Information Services Manager).

## Procédure

Pour désactiver l’inscription via le protocole http, il faudra le désactiver à l’aide de la console IIS (Internet Information Services Manager). La checkbox **Exiger SSL** est disponible en suivant le chemin suivant :

NomDuDomaine > Sites > NomDuSite > CertSrv

Afin d’activer la protection étendue pour l’authentification, dans la console ISS, vous pourrez choisir Exiger l’EPA dans les options avancées suivantes :

Pour l’inscription Web de l'autorité de certification :

NomDuDomaine > Sites > NomDuSite > CertSrv > Windows Authentification > Advanced Settings

Pour le Service web d'inscription de certificats :  
NomDuDomaine > Sites > <NOM CA>\_CES\_Kerberos > Windows Authentification > Advanced Settings

Après avoir activé l’option EPA, il est important de mettre à jour le fichier de configuration suivant en ajoutant la propriété **<extendedProtectionPolic*y*>** avec la valeur **Toujours** dans le fichier suivant :

<%windir%>\systemdata\CES\<CA Name>\_CES\_Kerberos\web.config  
  
extrait du fichier modifié :

<binding name="TransportWithHeaderClientAuth">

<security mode="Transport">

<transport clientCredentialType="Windows">

<extendedProtectionPolicy policyEnforcement="Always" />

</transport>

<message clientCredentialType="None" establishSecurityContext="false" negotiateServiceCredential="false" />

</security>

<readerQuotas maxStringContentLength="131072" />

</binding>

Afin de désactiver l’authentification NTLM sur les contrôleurs de domaines et sur les serveurs AD CS il est possible de déployer une GPO locale disponible dans Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options avec l’option Network security: Restrict NTLM: Incoming NTLM traffic sur Deny All Accounts ou Deny All domain accounts

Pour désactiver l’authentification NTLM pour l’IIS sur les serveurs AD CS en indiquant **Negotiate:Kerberos** dans la fenêtre suivante

Pour l’inscription Web de l'autorité de certification :

NomDuDomaine > Sites > NomDuSite > CertSrv > Windows Authentification Providers

Pour le Service web d'inscription de certificats :  
NomDuDomaine > Sites > <NOM CA>\_CES\_Kerberos > Windows Authentification > Providers

Attention, toute modification dans la console IIS nécessite le redémarrage afin de charger les changements et d’appliquer les modifications. Pour ce faire la commande suivante arrête tous les services actuellement lancés et les relances :

Iisreset /restart

Documentation :

* <https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>
* <https://learn.microsoft.com/fr-fr/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-ntlm-authentication-in-this-domain>