# Interface d’inscription des certificats accessible avec HTTP

ID METSYS : 32  
ID PingCastle : [A-CertEnrollHttp](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)

Charge de travail : 0.5 jour  
Difficulté : 1 - Requière quelques connaissances sur l'anomalie

****Description****

La PKI Windows, également appelée Services de certificats Active Directory (ADCS), peut être utilisée pour demander des certificats. Deux services peuvent être utilisés : l'inscription web de l'autorité de certification (WebEnrollment) et le service web d'inscription des certificats (CES). Les certificats fournis par ces services peuvent être utilisés avec Kerberos pour se connecter.

Étant donné que ce service peut délivrer des certificats pour les contrôleurs de domaine, il peut être considéré comme faisant partie du Tier 0. En tant que service hérité, les mécanismes visant à interdire le relais d'informations d'identification ne sont pas appliqués par défaut. Si un attaquant parvient à relayer des informations d'identification privilégiées (par exemple, avec l'attaque « PetitPotam »), il peut les utiliser pour prendre le contrôle du domaine.

****Recommandation****

L'accès à l'inscription des certificats via HTTP devrait être désactivé.

Cela peut être réalisé en ouvrant la console IIS sur le serveur d'inscription. Si le service mentionné en détail est « WebEnrollment », l'URL est « certsrv », sinon elle se termine par « CES\_Keberos ».

Dans les paramètres de liaison (lien à droite), conservez la liaison HTTPS et supprimez la liaison HTTP.