# Autorité de certification AD avec inscription Web

ID METSYS : 5  
ID PurplKnight : [AD Certificate Authority with Web Enrollment - PetitPotam and ESC8](https://www.purple-knight.com/fr/security-indicators/)

Charge de travail : 0.5 jour  
Difficulté : 2 - Requière quelques connaissances sur l'infrastructure et l'anomalie qu'elle contient

****Description****

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. Un exemple d'une telle attaque a été présenté en juillet 2021 lorsqu'elle était combinée avec la coercition d'authentification « PetitPotam » sur MS-EFSRPC. L'impact d'une telle attaque peut être une élévation de privilèges vers un administrateur de domaine à partir d'un accès réseau uniquement.

****Recommandation****

Selon les recommendations de Microsoft, assurez-vous que l'EPA est activé et que l'authentification NTLM est désactivée sur tous les serveurs AD CS. Pour plus d'informations, consultez les informations de [mitigation de MS](https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429).