# Utilisateurs principaux avec SPN ne prenant pas en charge le chiffrement AES sur Kerberos

ID METSYS : 24  
ID PingCastle : [P-Kerberoasting](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)  
ID PurplKnight : [Primary users with SPN not supporting AES encryption on Kerberos](https://www.purple-knight.com/fr/security-indicators/), [Privileged users with ServicePrincipalNames defined](https://www.purple-knight.com/fr/security-indicators/), [Users with ServicePrincipalName defined](https://www.purple-knight.com/fr/security-indicators/)  
ID ANSSI : [vuln1\_spn\_priv](https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#spn_priv)

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

****Description****

Pour accéder à un service à l'aide de Kerberos, un utilisateur demande un ticket (appelé TGS) au contrôleur de domaine spécifique au service. Ce ticket est chiffré à l'aide d'une dérivation du mot de passe du service, mais il peut être découvert par force brute pour récupérer le mot de passe d'origine.

Tout compte ayant l'attribut SPN renseigné est considéré comme un compte de service. Étant donné que n'importe quel utilisateur peut demander un ticket pour un compte de service, ces comptes peuvent avoir leur mot de passe récupéré. De plus, il est connu que les services n'ont pas leur mot de passe modifié régulièrement et utilisent des mots bien connus.

Le chiffrement AES est plus fort que le chiffrement RC4. Configurer les utilisateurs principaux avec SPN pour prendre en charge le chiffrement AES ne permettra pas de contrer des attaques telles que le « Kerberoasting », mais cela force l'utilisation d'AES par défaut, ce qui signifie qu'il est possible de surveiller les attaques de rétrogradation du chiffrement vers RC4 (attaques « Kerberoasting »).

****Recommandation****

Si le compte est un compte de service, le service devrait être supprimé du groupe privilégié ou avoir un processus de changement de mot de passe régulier.

Si l'utilisateur est une personne, l'attribut SPN du compte devrait être supprimé. Dans la mesure du possible, utilisez des comptes de service gérés par groupe (Group Managed Service Accounts) plutôt que des utilisateurs réguliers

La meilleure pratique consiste à activer la prise en charge du chiffrement AES sur les comptes de service. Suivez les [recommendations de Microsoft.](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-configure-encryption-types-allowed-for-kerberos)