# Dernière mise-à-jour du mot-de-passe Kerberos

ID METSYS : 3  
ID PingCastle : [A-Krbtgt](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)  
ID PurplKnight : [Kerberos krbtgt account with old password](https://www.purple-knight.com/fr/security-indicators/)  
ID ANSSI : [vuln2\_krbtgt](https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#krbtgt)

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

****Description****

Ce mot de passe peut être utilisé pour signer chaque ticket Kerberos. Une surveillance étroite de celui-ci atténue souvent considérablement le risque d'attaques par golden ticket.

Kerberos est un protocole d'authentification. Il utilise un secret, stocké sous la forme du mot de passe du compte « krbtgt », pour signer ses tickets. Si le hachage du mot de passe du compte « krbtgt » est récupéré, il peut être utilisé pour générer des tickets d'authentification à volonté.

Pour atténuer cette attaque, il est recommandé de changer le mot de passe « krbtgt » entre 40 jours et 6 mois. Si ce n'est pas le cas, chaque sauvegarde effectuée jusqu'au dernier changement de mot de passe du compte « krbtgt » peut être utilisée pour émettre des golden tickets, compromettant l'ensemble du domaine.

La récupération de ce secret est l'une des priorités les plus élevées lors d'une attaque, car ce mot de passe est rarement modifié et offre une porte dérobée à long terme. De plus, cette attaque peut être réalisée en utilisant l'ancien mot de passe du compte « krbtgt ». C'est pourquoi le mot de passe « krbtgt » doit être changé deux fois pour invalider toute fuite.

**Recommandation**

Le mot de passe du compte « krbtgt » doit être changé deux fois pour invalider l'attaque par golden ticket. Attention : deux changements du mot de passe « krbtgt » non répliqués sur les contrôleurs de domaine peuvent entraîner leur dysfonctionnement. Vous devriez attendre au moins 10 heures entre chaque changement de mot de passe « krbtgt » (c'est la durée de vie d'un ticket).

Il existe plusieurs possibilités pour changer le mot de passe « krbtgt ». Premièrement, un script Microsoft peut être exécuté afin de garantir la réplication correcte de ces secrets. Deuxièmement, une méthode plus manuelle consiste essentiellement à réinitialiser le mot de passe manuellement une fois, puis à attendre 3 jours (ce délai permet de garantir la sécurité de la réplication), puis à le réinitialiser à nouveau. C'est la méthode la plus sûre car elle garantit que le mot de passe n'est plus utilisable par l'attaque par golden ticket.