# Utilisateurs authentifiés pouvant créer des enregistrements DNS

ID METSYS : 27  
ID PingCastle : [A-DnsZoneAUCreateChild](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)

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

****Description****

Lorsqu'un ordinateur est joint à un domaine, un enregistrement DNS est créé dans la zone DNS pour permettre à l'ordinateur de mettre à jour ses paramètres DNS. Par conception, Microsoft a choisi d'accorder au groupe « Utilisateurs authentifiés » (c'est-à-dire tous les ordinateurs et utilisateurs) le droit de créer des enregistrements DNS. Une fois créé, seul le propriétaire conserve le droit de modifier le nouvel objet.

La vulnérabilité réside dans le fait que des enregistrements DNS spécifiques peuvent être créés pour effectuer des attaques de type « homme du milieu ». Un exemple est la création d'un enregistrement générique (un enregistrement avec le nom « \* »), d'un enregistrement DNS de basculement ou l'anticipation de la création d'un enregistrement DNS avec les permissions adéquates.

****Recommandation****

À ce jour, cette règle est considérée comme « informative » car la configuration par défaut où les utilisateurs authentifiés peuvent créer des enregistrements DNS est considérée comme sûre. La raison de cette classification est qu'aucune exploitation de cette vulnérabilité n'a été signalée.

L'amélioration proposée consiste à remplacer l'identité à qui le droit de créer des enregistrements DNS (permission « CreateChild ») a été accordé, en passant des « Utilisateurs authentifiés » aux « Ordinateurs du domaine ». Pour effectuer cette modification, vous devez éditer les autorisations de la zone DNS dont l'objet se trouve dans le conteneur « CN=MicrosoftDNS,DC=DomainDnsZones ».

Il convient de noter que si une élévation de privilèges se produit sur un ordinateur, un attaquant peut se faire passer pour le compte de cet ordinateur et contourner cette mesure d'atténuation. La meilleure mesure d'atténuation consiste à créer manuellement les enregistrements DNS dans le cadre du processus de jointure au domaine et à révoquer les autorisations accordées aux Utilisateurs authentifiés.