# SMB v1 activé sur des contrôleurs de domaines

ID METSYS : 31  
ID PingCastle : [S-SMB-v1](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)

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

****Description****

Un attaquant peut provoquer une exécution de code arbitraire à distance, un déni de service et un contournement de la politique de sécurité en exploitant une faille du protocole SMB v1

****Recommandation****

Il est recommandé de désactiver le protocole SMB v1 sur les contrôleurs de domaine, les serveurs et stations du domaine.

En prérequis, il faut supprimer les OS obsolètes (2000/2003/2008/XP/Vista/7/10 < « 1709 ») du domaine sinon ils ne pourront plus se connecter au partage SYSVOL sur les DC pour appliquer les GPO.