# Confiance de domaine envers un domaine tiers sans quarantaine

ID METSYS : 20  
ID PurplKnight : [Domain trust to a third-party domain without quarantine](https://www.purple-knight.com/fr/security-indicators/)  
ID ANSSI : [vuln1\_trusts\_domain\_ notfiltered](https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#trusts_domain_ notfiltered)

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

****Description****

Un attaquant ayant compromis le domaine distant peut usurper l'identité de n'importe quel utilisateur ou machine sur le domaine local (à l'exception des comptes ayant un RID inférieur à 1000, excluant les comptes et groupes intégrés). Cet attaquant peut ainsi accéder à toutes les ressources du domaine local. Si un chemin de contrôle dangereux est exposé à un compte « usurpable » (pratiquement tout compte autre que les comptes intégrés), l'attaquant pourrait également escalader ses privilèges jusqu'aux « Administrateurs de domaine » et compromettre l'ensemble de la forêt.

****Recommandation****

À moins que la migration de domaine ne soit en cours, utilisez la commande suivante pour activer la mise en quarantaine de la confiance :

NETDOM TRUST /domain: /Quarantine yes