# Mitigation pour la « CVE-2021-42291 » a été activée

ID METSYS : 51  
ID PingCastle : [A-DsHeuristicsLDAPSecurity](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)  
ID ANSSI : [vuln3\_dsheuristics\_bad](https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#dsheuristics_bad)

Charge de travail : 1 jour  
Difficulté : 2 - Requière quelques connaissances sur l'infrastructure et l'anomalie qu'elle contient

****Description****

Le comportement d'un annuaire Active Directory peut être contrôlé via l'attribut « DsHeuristics » de « CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration ». Un paramètre stocké dans cet attribut, dont les valeurs sont « LDAPAddAutZVerifications » et « LDAPOwnerModify », peut être configuré pour modifier la mitigation de la « CVE-2021-42291 ».

La mise à jour « KB5008383 » a introduit des modifications dans le descripteur de sécurité par défaut des conteneurs d'ordinateurs afin d'ajouter une journalisation et de limiter la création d'ordinateurs sans être administrateur. En effet, il est recommandé de ne pas permettre à n'importe qui de créer des comptes d'ordinateurs, car ils peuvent être utilisés pour abuser de Kerberos ou effectuer des attaques de relais.

Les mitigations pour la « CVE-2021-42291 » consistent en 3 choix à définir sur 2 paramètres. Ils sont appelés « LDAPAddAutZVerifications » et « LDAPOwnerModify » et correspondent respectivement au 28e et au 29e caractère de cette chaîne. Pour les valeurs attendues :

• Avec la valeur 0 (par défaut), cela active un mécanisme de journalisation supplémentaire.

• Avec la valeur 1 (recommandée), cela renforce les autorisations de sécurité, en particulier pour exiger une action de l'administrateur de domaine lors d'actions inhabituelles.

• Avec la valeur 2 (non recommandée), cela désactive le mécanisme de journalisation qui a été ajouté par défaut et n’active pas les nouvelles autorisations de sécurité.

****Recommandation****

La manière la plus simple et la plus rapide de corriger ce problème est de remplacer le 28e et le 29e caractère de l'attribut « DsHeuristics ». Les valeurs de « LDAPAddAutZVerifications » et « LDAPOwnerModify » doivent être définies sur 1.

Suivez la procédure intégrée à la mise à jour « KB5008383 » pour appliquer cette mitigation et modifier la valeur de « DsHeuristics ».

Note : Vous devez faire attention aux caractères de contrôle en 10e et 20e position pour éviter des modifications indésirables de l'attribut « DsHeuristics ». Typiquement, si « DsHeuristics » est vide, la nouvelle valeur attendue est « 00000000010000000002000000011 ».