

La base de données de signatures Windows Defender vide après la désinstallation de Norton Antivirus entraîne une erreur de posture ISE

Table des matières

Problème

Les terminaux Windows 11 25H2 se connectant via un VPN ne sont pas conformes aux contrôles de position ISE et sont marqués comme non conformes, ce qui empêche l'authentification et l'accès aux ressources réseau. Le terminal répond aux exigences de la règle ISE, mais signale tout de même « l'utilisateur ne répond pas aux exigences » après la connexion VPN.

La vérification de la position échoue spécifiquement pour la validation de la version de définition antivirus de Windows Defender avec cette erreur :

```
[csc_iseposture]Function: CheckOpswat::CheckOpswatProd Thread Id: 0x277C File: CheckOpswat.cpp Line: 27
```

L'agent de posture signale que Windows Defender a une version de définition et une date de définition vides égales à 0, ce qui entraîne l'échec de la condition AUC_WIN11_IT.

Environnement

- Identity Services Engine (ISE) 3.3
- Terminaux Windows 11 25H2
- Cisco Secure Client avec module de posture ISE
- Module de conformité ISEC version 4.3.5626.8192
- Windows Defender version 4.18.25080.5

- Norton 360 antivirus a déjà été installé et désinstallé
- Connexion VPN avec application de la position ISE activée

Résolution

La résolution implique la désinstallation de Norton, puis la mise à jour manuelle des signatures Windows Defender et la compréhension du comportement de coexistence entre l'antivirus tiers et Windows Defender.

Étape 1: Mettre à jour les signatures Windows Defender

1.- Accédez aux paramètres de sécurité Windows et mettez à jour manuellement la base de données de signatures :

2.- Accédez à Paramètres → Confidentialité et sécurité → Sécurité Windows → Protection contre les virus et les menaces → Mises à jour de protection contre les virus et les menaces → Rechercher les mises à jour.

3.- Attendez que la version Security Intelligence affiche une valeur non vide et un horodatage actuel avant de procéder à la validation de la position.

Étape 3: Vérifier la conformité des postures

Après avoir mis à jour les signatures, reconnectez-vous au VPN et vérifiez que la vérification de la position a réussi. La version de l'intelligence de sécurité doit maintenant afficher une valeur valide au lieu d'être vide.

Considérations importantes relatives aux antivirus tiers

Lorsqu'un antivirus tiers est installé et correctement enregistré auprès du Centre de sécurité Windows, Microsoft Windows met intentionnellement Windows Defender en mode passif pour

éviter les conflits. En mode passif, Defender ne publie pas ses données d'actualisation des signatures via l'API du Centre de sécurité Windows/WMI lue par OPSWAT, ce qui entraîne l'échec des vérifications de position.

Pour éviter ce problème, désinstallez l'application tierce que Windows met en mode actif. Si vous devez réinstaller Norton ou un autre logiciel antivirus tiers, sachez que le point d'extrémité redevient non conforme.

Motif

La cause principale est que la base de données de signatures Windows Defender devient obsolète lorsqu'un antivirus tiers (Norton) est la solution antivirus principale. Lors de l'installation de Norton, Windows a intentionnellement gardé le magasin de définitions de Defender périmé, car le logiciel antivirus en mode passif ne reçoit pas les mises à jour planifiées. Après la désinstallation de Norton, Windows Defender est devenu l'antivirus principal, mais sa base de données de signatures est restée vide car la première extraction de signature est mise en file d'attente derrière Windows Update et ne s'exécute automatiquement que sur son prochain déclencheur planifié ou lorsqu'elle est forcée manuellement par l'utilisateur.

La méthode SDK OPSWAT v4 1001 (GetDefinitionState) retourne une charge utile vide lorsque le magasin de définitions locales Defender est vide, ce qui amène l'agent de posture ISE à transmettre une version de définition vide à ISE. ISE compare ensuite cette valeur vide au seuil de stratégie et marque le terminal comme non conforme.

Autres informations utiles

- [Guide d'administration de Cisco Secure Client - Considérations relatives aux logiciels tiers](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.