Dépannage de la position sans agent ISE non déclenchée après réauthentification de session

Table des matières

Problème

La fonctionnalité de posture sans agent d'Identity Services Engine (ISE) 3.3 ne parvient pas à se déclencher après les événements de réauthentification de session. Lors de l'authentification initiale, la position sans agent fonctionne correctement et les terminaux deviennent conformes. Cependant, lorsque la réauthentification se produit, les points de terminaison reçoivent des événements de mise à jour provisoire de comptabilité RADIUS au lieu d'événements de début de comptabilité, ce qui empêche l'appel du flux de posture sans agent. Par conséquent, les terminaux correspondent à une stratégie de posture inconnue et restent dans un état de posture inconnu, ce qui a un impact sur l'accès au réseau pour les périphériques affectés.

Le problème se manifeste avec des terminaux bloqués dans l'état « Position en attente » ou « Inconnu » après une nouvelle authentification, avec environ 800 terminaux sur 1200 affectés dans l'environnement signalé. L'analyse du journal montre que pendant la réauthentification, ISE reçoit les événements ACCOUNTING_UPDATE avec agentlessEnabled=true, mais que le flux de posture n'est pas appelé à nouveau pour l'ID de session existant.

Environnement

- Identity Services Engine (ISE) version 3.3 Patch 4
- Authentification 802.1X filaire avec contournement d'authentification MAC (MAB)
- Configuration de posture sans agent activée
- Temporisateurs de réauthentification de session configurés (délai d'attente de 420 secondes)
- Commutateurs Cisco Catalyst en tant que périphériques d'accès réseau
- Environ 1 200 terminaux dans l'environnement

Résolution

Ce comportement est attendu et prévu dans ISE. La position sans agent est uniquement déclenchée par les événements de démarrage de la comptabilité RADIUS et ne doit pas être réappelée par les événements de mise à jour provisoire de la comptabilité lors de la réauthentification de session lorsque l'adresse IP tramée reste inchangée.

Analyse technique

Le chemin de code ISE NetAccessEventHandler réarme uniquement le flux de posture sans agent sur les nouveaux paquets RADIUS Accounting-Start. Lors de la réauthentification, les périphériques réseau envoient généralement des paquets Accounting Interim-Update avec le même ID de session de compte, ce qui entraîne le renvoi de false par la fonction shouldInvokePostureFlow(), ce qui empêche la réévaluation de la position.

Consignez les preuves indiquant le comportement :

Authentification Initiale (Déclenchement De La Position Sans Agent) :

```
2026-04-01 11:28:20,466 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle
2026-04-01 11:28:20,466 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle
```

Réauthentification (position sans agent non déclenchée) :

```
2026-04-01 11:35:37,669 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle
```

Solution recommandée

Pour limiter l'impact de ce comportement, configurez les paramètres de location de position afin de maintenir la conformité des terminaux pendant les scénarios de réauthentification :

Étape 1: Configurez la durée de bail de position appropriée dans les politiques de position ISE pour garantir que les terminaux ne perdent pas l'accès réseau entre les évaluations de position.

Étape 2: Surveillez l'état des terminaux et ajustez les compteurs de crédit-bail en fonction des exigences de sécurité de votre entreprise et de la fréquence de réauthentification.

Motif

Ce comportement est attendu et documenté dans l'ID de bogue Cisco CSCwu48086. La position sans agent dans ISE est conçue pour se déclencher uniquement sur les événements RADIUS Accounting Start et n'est pas déclenchée par les événements Interim Accounting Update. Lors de la réauthentification de session, les périphériques d'accès réseau envoient des mises à jour provisoires de comptabilité avec la même adresse IP et le même ID de session tramés, qui ne réappellent pas le processus d'évaluation de la position sans agent. Le code ISE vérifie spécifiquement les nouvelles sessions (événements ACCOUNTING_START) avant de lancer des flux de posture sans agent.

Autres informations utiles

- ID de bogue Cisco CSCwu48086
- 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.