Risoluzione dei problemi relativi alla postura senza agente ISE che non viene attivata dopo la riautenticazione della sessione

Sommario

Problema

La funzionalità di postura senza agente in Identity Services Engine (ISE) 3.3 non viene attivata dopo gli eventi di riautenticazione della sessione. Durante l'autenticazione iniziale, la postura senza agente funziona correttamente e gli endpoint diventano conformi. Tuttavia, quando si verifica la riautenticazione, gli endpoint ricevono gli eventi di aggiornamento intermedio di RADIUS Accounting anziché gli eventi di avvio di accounting, che impediscono il richiamo del flusso di postura senza agente. Di conseguenza, gli endpoint corrispondono a una policy di postura sconosciuta e rimangono in uno stato di postura sconosciuto, con un impatto sull'accesso alla rete per i dispositivi interessati.

Il problema si manifesta con gli endpoint bloccati nello stato "Postura in sospeso" o "Sconosciuto" dopo la riautenticazione, con circa 800 endpoint su 1200 interessati nell'ambiente di report. L'analisi del registro mostra che durante la riautenticazione, ISE riceve gli eventi ACCOUNTING_UPDATE con agentlessEnabled=true ma il flusso di postura non viene richiamato nuovamente per l'ID sessione esistente.

Ambiente

- Patch 4 per Identity Services Engine (ISE) versione 3.3
- Autenticazione 802.1X cablata con MAC Authentication Bypass (MAB)
- Configurazione della postura senza agente abilitata
- Timer di riautenticazione della sessione configurati (timeout di 420 secondi)
- Switch Cisco Catalyst come dispositivi di accesso alla rete
- Circa 1200 endpoint nell'ambiente

Risoluzione

Questo è il comportamento previsto e previsto da ISE. La postura senza agente viene attivata solo dagli eventi di avvio dell'accounting RADIUS e non deve essere richiamata nuovamente dagli eventi di aggiornamento intermedio dell'accounting durante la riautenticazione della sessione quando l'indirizzo IP con frame rimane invariato.

Analisi tecnica

Il percorso del codice ISE NetAccessEventHandler esegue solo il riarmo del flusso di postura senza agente sui pacchetti RADIUS Accounting-Start freschi. Durante la riautenticazione, i dispositivi di rete in genere inviano pacchetti di accounting per l'aggiornamento interinale con lo stesso Act-Session-Id. In questo modo, la funzione shouldInvokePostureFlow() restituisce false e ciò impedisce la rivalutazione della postura.

Registra evidenza del comportamento:

Autenticazione iniziale (postura senza agente attivata):

```
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
```

Riautenticazione (postura senza agente non attivata):

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

Soluzione consigliata

Per ridurre l'impatto di questo comportamento, configurare le impostazioni di lease della postura per mantenere la conformità dell'endpoint durante gli scenari di riautenticazione:

Passaggio 1: Configurare la durata lease della postura appropriata nelle policy di postura ISE in modo che gli endpoint non perdano l'accesso alla rete tra le valutazioni della postura.

Passaggio 2: Monitorare lo stato della postura degli endpoint e regolare i timer di lease in base ai requisiti di sicurezza dell'organizzazione e alla frequenza di riautenticazione.

Causa

Questo è il comportamento previsto documentato nell'ID bug Cisco CSCwu48086. La postura senza agente in ISE è progettata per attivare solo gli eventi di avvio dell'accounting RADIUS e non è attivata dagli eventi di aggiornamento dell'accounting provvisorio. Durante la riautenticazione della sessione, i dispositivi di accesso alla rete inviano aggiornamenti intermedi di accounting con lo stesso indirizzo IP con frame e ID sessione, che non richiamano nuovamente il processo di valutazione della postura senza agente. Il codice ISE controlla specificamente le nuove sessioni (eventi ACCOUNTING_START) prima di avviare i flussi di postura senza agente.

Contenuto correlato

- Cisco, ID bug CSCwu48086
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).