Solucionar problemas de não disparo de postura sem agente do ISE após a reautenticação da sessão

Contents

Problema

A funcionalidade de postura sem agente no Identity Services Engine (ISE) 3.3 falha ao disparar após eventos de reautenticação de sessão. Durante a autenticação inicial, a postura sem agente funciona corretamente e os endpoints se tornam compatíveis. No entanto, quando ocorre uma nova autenticação, os pontos de extremidade recebem eventos de Atualização Provisória de Contabilização RADIUS em vez de eventos de Início de Contabilização, fazendo com que o fluxo de postura sem agente não seja chamado. Como resultado, os endpoints correspondem a uma política de postura desconhecida e permanecem em um estado de postura desconhecida, afetando o acesso à rede para os dispositivos afetados.

O problema se manifesta com pontos finais presos no status "Postura Pendente" ou "Desconhecido" após a reautenticação, com aproximadamente 800 dos 1200 pontos finais afetados no ambiente relatado. A análise de log mostra que, durante a reautenticação, o ISE recebe eventos ACCOUNTING_UPDATE com agentlessEnabled=true, mas o fluxo de postura não é chamado novamente para a ID de sessão existente.

Ambiente

- Patch 4 do Identity Services Engine (ISE) versão 3.3
- Autenticação 802.1X com fio com desvio de autenticação MAC (MAB)
- Configuração de postura sem agente habilitada
- Temporizadores de reautenticação de sessão configurados (tempo limite de 420 segundos)
- Switches Cisco Catalyst como dispositivos de acesso à rede
- Aproximadamente 1200 endpoints no ambiente

Resolução

Esse comportamento é esperado e projetado no ISE. A postura sem agente é acionada apenas por eventos de início de contabilização RADIUS e não deve ser invocada novamente por eventos de atualização provisória de contabilização durante a reautenticação da sessão quando o endereço IP com quadros permanecer inalterado.

Análise técnica

O caminho de código NetAccessEventHandler do ISE rearma apenas o fluxo de postura sem agente em pacotes Accounting-Start RADIUS novos. Durante a reautenticação, os dispositivos de rede normalmente enviam pacotes Accounting Interim-Update com o mesmo Acct-Session-Id, o que faz com que a função shouldInvokePostureFlow() retorne false, evitando a reavaliação da postura.

Registrar evidência que mostra o comportamento:

Autenticação Inicial (Disparada Por Postura Sem Agente):

```
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
```

Reautenticação (postura sem agente não disparada):

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

Solução recomendada

Para atenuar o impacto desse comportamento, defina as configurações de aluguel de postura para manter a conformidade do endpoint durante cenários de reautenticação:

Passo 1: Configure a duração de aluguel de postura apropriada nas políticas de postura do ISE para garantir que os endpoints não percam o acesso à rede entre as avaliações de postura.

Passo 2: Monitore o status da postura do endpoint e ajuste os temporizadores de leasing com base nos requisitos de segurança e na frequência de reautenticação da sua organização.

Causa

Este é o comportamento esperado documentado na ID de bug Cisco CSCwu48086. A postura sem agente no ISE foi projetada para disparar somente em eventos de início de contabilidade RADIUS e não é disparada por eventos de atualização de contabilidade provisórios. Durante a reautenticação da sessão, os dispositivos de acesso à rede enviam Atualizações Provisórias de Contabilização com o mesmo endereço IP Enquadrado e ID da sessão, que não invocam novamente o processo de avaliação da postura sem agente. O código ISE verifica especificamente novas sessões (eventos ACCOUNTING_START) antes de iniciar fluxos de postura sem agente.

Conteúdo relacionado

- ID de bug Cisco CSCwu48086
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.