Atualização do Snort Engine Bloqueada Durante Atualização de FTD Devido à Detecção de Política Personalizada

Contents

Problema

Durante uma atualização de FTD da versão 7.2 para 7.4.4 em um HA FPR-4115 gerenciado pelo FMC, a atualização do mecanismo Snort para o Snort 3 é bloqueada com mensagens de erro indicando falha na conversão das regras personalizadas do Snort 2 ou no uso de políticas personalizadas de intrusão ou análise de rede. A mensagem de erro específica informa: "Não é possível atualizar para o Snort 3. O dispositivo usa pelo menos uma política de intrusão personalizada ou uma política de análise de rede." Uma mensagem de falha mais detalhada refere-se à incapacidade de converter regras personalizadas do Snort 2 e aponta para /var/sf/htdocs/ips/snort.rej para obter detalhes. A preocupação é se esse erro impediria a migração para o Snort 3 e afetaria a funcionalidade de inspeção.

Ambiente

- Cisco Secure Firewall Firepower versão 7.3
- Firepower Management Center (FMC) versão 7.7.11
- Dispositivos FTD em configuração de alta disponibilidade (HA)
- Hardware: FPR-4115
- Caminho de atualização: FTD 7.2 a 7.4.4
- VDB na versão mais recente antes da atualização
- Seção Regras locais em Objetos > Regras de intrusão > Snort 2 All Rules está vazia

Resolução

A mensagem de erro que bloqueia a atualização do mecanismo Snort é um comportamento documentado relacionado ao bug da Cisco ID CSCwn46794 e não representa um bloqueador funcional quando não existem regras personalizadas de Snort 2.

Etapas de verificação

Etapa 1: Verifique o status das regras personalizadas do Snort 2

Navegue até a interface do FMC e verifique se há regras Snort 2 personalizadas:

`Objetos > Regras de intrusão > Snort 2 Todas as regras > Regras locais`

Etapa 2: Confirmar a versão do VDB

Verifique se o Banco de Dados de Vulnerabilidade (VDB) tem a versão mais recente antes de continuar com a atualização.

Etapa 3: Revise os detalhes do erro

Verifique as informações detalhadas do erro no arquivo referenciado:

`/var/sf/htdocs/ips/snort.rej`

Processo de atualização

Quando a seção "Regras locais" for confirmada como vazia (não há regras personalizadas do Snort 2), a atualização poderá continuar apesar da mensagem de erro. O erro de bloqueio é um falso positivo nesse cenário e não indica regras personalizadas reais que precisam de conversão.

Etapa 1: Continue com a atualização do Snort 3

Continue com o processo de atualização do FTD para a versão 7.4.4, que inclui a atualização do mecanismo Snort 3.

Etapa 2: Validação Pós-Atualização

Depois que a atualização for concluída com êxito, teste o fluxo de tráfego para confirmar o comportamento esperado com o mecanismo Snort 3.

Etapa 3: Monitorar o desempenho do sistema

Verifique se a funcionalidade de inspeção opera conforme esperado com o novo mecanismo Snort 3.

Causa

A mensagem de bloqueio de atualização é um comportamento documentado associado ao bug da Cisco ID CSCwn46794. Esse bug faz com que o sistema exiba uma mensagem de erro sobre políticas de intrusão personalizadas ou políticas de análise de rede, mesmo quando não existem regras Snort 2 personalizadas reais que requerem conversão. A mensagem de erro aparece como um falso positivo quando a seção Regras Locais está vazia, mas a validação de pré-atualização do sistema identifica incorretamente a presença de políticas personalizadas.

Conteúdo relacionado

- ID de bug Cisco CSCwn46794

- ID de bug Cisco CSCwk07199
- 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.