Identificar e solucionar problemas de eventos de intrusão do FMC mostrando o impacto=Desconhecido

Contents

Problema

Após a implantação de um novo Firewall Management Center (FMC) e a atualização para a versão 7.7.12, todos os eventos de invasão exibem "Impact=Unknown" em vez dos valores de impacto esperados. Isso evita que os mecanismos de alerta apropriados sejam acionados, já que o campo de impacto é necessário para a configuração de alertas.

Ambiente

- FMC versão 7.7.12. Outras versões de software também podem ser afetadas.
- Política de intrusão no modo de prevenção ou detecção.

Resolução

A resolução desse problema envolve a verificação e a configuração do escopo da política de detecção para incluir todos os endereços IP relevantes onde os eventos de invasão são gerados.

Etapa 1. Identificar os endereços IP afetados

Analise os eventos de intrusão que estão mostrando "Impacto=Desconhecido" e identifique os

endereços IP específicos envolvidos nesses eventos. Documente esses endereços IP para comparação com a configuração atual da política de descoberta.

Etapa 2. Rever a Configuração Atual da Política de Descoberta

Navegue até FMC Policies > Network Discovery (em versões mais recentes é Policies > Advanced > Network Discovery) e examine as configurações atuais da política de descoberta para determinar quais intervalos de endereços IP ou sub-redes estão atualmente incluídos no escopo de descoberta.

Etapa 3. Atualizar Escopo da Política de Descoberta

Modifique a configuração da política de detecção para incluir todos os endereços IP onde ocorrem eventos de invasão. Certifique-se de que o escopo da política de descoberta abranja todos os segmentos de rede onde você espera receber eventos de invasão com uma avaliação de impacto apropriada.

Etapa 4. Implantar Alterações de Configuração

Implante a configuração atualizada da política de descoberta em todos os dispositivos gerenciados para garantir que as alterações tenham efeito em toda a infraestrutura de segurança.

Etapa 5. Verificar o Preenchimento do Campo de Impacto

Monitore novos eventos de invasão para confirmar se o campo de impacto agora está sendo preenchido com valores apropriados em vez de "Desconhecido".

Causa

Os eventos de intrusão que mostram "Impact=Unknown" foram causados por um problema de configuração em que os endereços IP afetados não foram incluídos em nenhuma política de detecção no FMC. Quando os endereços IP estão fora do escopo das políticas de descoberta configuradas, o FMC não pode avaliar corretamente o impacto de eventos de invasão para esses endereços, resultando no campo de impacto sendo preenchido com valores "Desconhecidos". Esse é um problema relacionado à configuração, e não um defeito de software ou hardware.

Conteúdo relacionado

- Níveis de impacto de evento de intrusão
- 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.