Verificar os caminhos de atualização direta do VDB e o impacto do tráfego no FMC

Contents

Problema

Ao executar por trás de atualizações do banco de dados de vulnerabilidade (VDB), os administradores precisam entender se as atualizações do VDB são cumulativas e se podem ignorar versões intermediárias.

Neste exemplo, a preocupação é ao atualizar do VDB versão 393 para a versão 427. Especificamente, há incerteza sobre se várias etapas de atualização são necessárias ou se um caminho de atualização direto é suportado. Além disso, surgem preocupações sobre possíveis interrupções de serviço durante a atualização do VDB e o subsequente processo de implantação da política.

Ambiente

- Software Secure Firewall Management Center (FMC) versão 7.4.2.4. Outras versões de software também são afetadas.
- Firewall Threat Defense (FTD) no FPR 2110. Outras plataformas de hardware também são afetadas.
- Versão VDB atual: 393. Outras versões de software também são afetadas.
- Versão do VDB de destino: 427. Outras versões de software também são afetadas.

Resolução

As atualizações do VDB no FMC são cumulativas, permitindo atualizações diretas de versões

mais antigas para versões mais novas sem exigir etapas intermediárias.

Processo de atualização do VDB

Você pode atualizar diretamente do VDB versão 393 para o VDB versão 427 sem nenhuma etapa de atualização de VDB intermediária. Começando com a versão 357 do VDB, a Cisco suporta a instalação de qualquer versão do VDB desde a linha de base do VDB na plataforma FMC.

Para fazer o download da versão mais recente do VDB, consulte Download de software.

Considerações sobre o impacto do serviço

O risco primário não está associado à instalação do VDB em si no FMC, mas sim à primeira implantação de política no FTD após a atualização do VDB. Na maioria dos casos, a primeira implantação após uma atualização de VDB reinicia o processo Snort, o que interrompe temporariamente a inspeção de tráfego.

Durante este período de interrupção:

- O tráfego pode cair ou passar sem inspeção adicional.
- O comportamento específico depende de como o FTD é configurado para lidar com o tráfego durante as reinicializações do processo.

Práticas recomendadas:

- Programar a parte de implantação da política durante uma janela de manutenção planejada.
- Coordenar-se com as operações de rede para minimizar o impacto sobre o usuário.
- Monitore o status do sistema durante e após o processo de implantação.

Causa

- Começando com o VDB 357, você pode instalar qualquer atualização de VDB desde o VDB de linha de base para o FMC.
- A instalação requer uma reimplantação de política para ativar as novas assinaturas de vulnerabilidade, o que aciona uma reinicialização do processo Snort em dispositivos FTD gerenciados. Essa reinicialização cria uma breve interrupção nos recursos de inspeção de tráfego enquanto o novo banco de dados é carregado e o mecanismo de inspeção é reinicializado.

Conteúdo relacionado

- Guia de administração do Cisco Secure Firewall Management Center - Atualizações do sistema
- Guia de configuração de dispositivos do Cisco Secure Firewall Management Center - Implantação
- 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.