Comportamento de Substituição da Ação de Aviso do Cisco Secure Access com Configurações de Bloqueio de IPS

Contents

Problema

Ao testar o comportamento Avisar em uma Política de acesso (Acesso à Internet) no Cisco Secure Access com IPS habilitado, os usuários experimentam um comportamento inesperado em que a ação Avisar parece substituir as configurações de bloqueio de IPS. Especificamente, ao acessar uma URL destinada a disparar uma assinatura de IPS (SERVER-WEBAPP /etc/passwd tentativa de acesso a arquivos, GID-SID: 1-1122), uma página de aviso é exibida e, após a confirmação do usuário, o acesso ao URL é permitido, apesar do IPS estar configurado para bloquear o tráfego.

A configuração inclui:

- Ação: Isolar
- Prevenção contra invasões (IPS): Enable
- IPS/Bloqueio
- Assinatura: SERVER-WEBAPP /etc/passwd tentativa de acesso a arquivos
- GID-SID: 1-1122

Os logs de pesquisa de atividades mostram entradas conflitantes:

- IPS: (IPS: bloqueio)
- WEB: (WEB: permitir - página de aviso exibida)
- WEB: (WEB: permitir - após acesso de aviso)

Ambiente

- Produto: Vantagem do Cisco Secure Internet Access
- Tecnologia: Acesso seguro
- Política de acesso configurada com a ação de Aviso e Acesso à Internet
- IPS habilitado com ação de bloqueio para assinaturas específicas

Resolução

Esse comportamento foi identificado como um defeito no Cisco Secure Access, em que a ação Avisar nas Políticas de Acesso tem precedência sobre as configurações do bloco IPS. O problema afeta a interação entre as ações de Aviso da política de acesso e a funcionalidade de bloqueio de IPS.

Etapas de verificação

Para verificar esse comportamento no seu ambiente:

Passo 1: Configurar a política de acesso com a ação Avisar e habilitar o bloqueio de IPS

- Definir ação para isolar com comportamento Avisar
- Habilitar prevenção contra invasões (IPS)
- Ação Configurar IPS com Bloqueio
- Aplicar assinatura específica (por exemplo, SERVER-WEBAPP /etc/passwd tentativa de acesso a arquivos, GID-SID: 1-1122)

Passo 2: Teste a configuração acessando uma URL que dispare a assinatura de IPS

```
https://example.com/etc/passwd
```

Passo 3: Observar o comportamento

- A página de aviso será exibida ao usuário
- O usuário pode continuar depois de confirmar o aviso
- O acesso à URL será permitido apesar da configuração do bloco de IPS

Passo 4: Verificar logs de pesquisa de atividade

- Verificar a presença de entradas de bloqueio de IPS e permissão da WEB
- Confirme se as entradas de log conflitantes indicam o defeito

Status atual

Este comportamento foi confirmado como um defeito em que a ação Avisar substitui as configurações do bloco IPS por design na implementação atual. O mesmo comportamento ocorre com assinaturas IPS diferentes de GID-SID: 1-1122, indicando que esse é um problema sistêmico que afeta todas as assinaturas de IPS quando as ações de aviso são configuradas.

Ainda não foram determinados um plano e um cronograma de correção para este defeito. As empresas que tiverem esse problema devem avaliar suas políticas de segurança e considerar configurações alternativas se for necessário um bloqueio de IPS rigoroso.

Causa

A causa raiz é um defeito no Cisco Secure Access em que o processamento da ação Aviso da política de acesso tem precedência sobre a aplicação do bloco IPS. Essa falha de design permite que os usuários ignorem os controles de segurança do IPS por meio do mecanismo de confirmação de aviso, anulando efetivamente a funcionalidade de bloqueio do IPS quando as ações de Aviso são configuradas.

A ID de bug Cisco CSCwt39270 está associada a este caso, embora a relação específica entre este bug e o comportamento observado de Aviso versus IPS exija investigação adicional.

Conteúdo relacionado

- 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.