Habilitação da característica ESA DHAP

ID do Documento: 117847

Atualizado em: junho 25, 2014

Contribuído por John Yu e por Robert Sherwin, engenheiros de TAC da Cisco.

Produtos Relacionados

- Dispositivo do Gerenciamento de segurança do índice de Cisco
- Cisco envia por correio eletrónico a ferramenta de segurança
- Ferramenta de segurança da Web de Cisco

Índice

Introdução

Este documento descreve como permitir a característica da prevenção do ataque da colheita do diretório (DHAP) na ferramenta de segurança do email de Cisco (ESA) a fim impedir ataques da colheita do diretório (DHAs).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco ESA
- AsyncOS

Componentes Utilizados

A informação neste documento é baseada em todas as versões de AsyncOS.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Um DHA é uma técnica que seja usada por spammer a fim encontrar endereços email válidos. Há duas técnicas principal que são usadas a fim gerar os endereços alvos esse DHA:

- O spammer cria uma lista de todas as combinações possíveis de letras e de números, e adiciona então o Domain Name.

- O spammer usa um ataque do dicionário padrão com a criação de uma lista que combine nomes, sobrenomes, e iniciais comuns.

O DHAP é uma característica suportada nas ferramentas de segurança do índice de Cisco que podem ser permitidas quando a validação da aceitação do Lightweight Directory Access Protocol (LDAP) é usada. A característica DHAP mantém-se a par do número de endereços destinatários inválidos de um remetente dado.

Uma vez que um remetente cruza um ponto inicial administrador-definido, o remetente está julgado ser não confiável, e o correio desse remetente é obstruído sem a geração do requisito de design de rede (NDR) ou do código de erro. Você pode configurar o ponto inicial baseado na reputação do remetente. Por exemplo, os remetentes não confiáveis ou suspeitos podem ter um baixo ponto inicial DHAP, e os remetentes confiados ou respeitáveis podem ter um ponto inicial alto DHAP.

Permita DHAP

A fim permitir a característica DHAP, navegue **para enviar políticas > tabela do acesso host (CHAPÉU) da** ferramenta de segurança satisfeita GUI e para selecionar **políticas do fluxo de correio**. Escolha a política que você deseja editar da coluna do **nome da política**.

O CHAPÉU tem quatro regras básicas do acesso que são usadas a fim atuar em cima das conexões dos host remotos:

- ACEITO: A conexão é aceitada, e a aceitação do email é restringida mais pelos ajustes do ouvinte. Isto inclui a tabela destinatária do acesso (para ouvintes públicos).

- **REJEIÇÃO**: A conexão é aceitada inicialmente, mas o cliente que as tentativas de conectar

recebem um cumprimento 4XX ou 5XX. Nenhum email é aceitado.

- **TCPREFUSE**: A conexão é recusada a nível TCP.
- **RELÉ**: A conexão é aceitada. Receber para todo o receptor é permitida e não forçada pela tabela destinatária do acesso. A assinatura das chaves do domínio está disponível somente em políticas do fluxo de correio do relé.

Na seção dos **limites do fluxo de correio da** política selecionada, o achado e ajustou a configuração da **prevenção do ataque da colheita do diretório (DHAP)** ajustando os receptores inválidos máximos pela hora. Você pode igualmente escolher personalizar os receptores inválidos máximos pelo código da hora e Máximo Inválido Receptor pelo texto da hora se você deseja assim.

Você deve repetir esta seção a fim configurar DHAP para políticas adicionais.

Assegure-se de que você submeta e comprometa todas as mudanças no GUI.

> **Note**: Cisco recomenda que você usa um número máximo entre cinco e dez para o **número máximo de receptores inválidos pela hora de um** ajuste do **host remoto**.

> **Note**: Para a informação adicional, refira o **Guia do Usuário de AsyncOS no** portal do apoio de Cisco.

Cisco relacionado apoia discussões da comunidade

Cisco apoia a comunidade é um fórum para que você faça e responda a perguntas, sugestões da parte, e colabora com seus pares.

Refira convenções dos dicas técnicas da Cisco para obter informações sobre das convenções usadas neste documento.

Atualizado em: junho 25, 2014
ID do Documento: 117847