Contenido

Introducción

Este documento describe cómo permitir a la característica de la prevención del ataque de recopilación de direcciones (DHAP) en el dispositivo de seguridad del correo electrónico de Cisco (ESA) para prevenir los ataques de recopilación de direcciones (DHA).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco ESA
- AsyncOS

Componentes Utilizados

La información en este documento se basa en todas las versiones de AsyncOS.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Un DHA es una técnica que es utilizada por los spammeres para localizar las direcciones de correo electrónico válidas. Hay dos técnicas principales que se utilizan para generar los direccionamientos las blancos ese DHA:

- El spammer crea una lista de todas las combinaciones posible. de cartas y de números, y después añade el Domain Name al final del fichero.

- El spammer utiliza un establecimiento de diccionario estándar con la creación de una lista que combine los primeros nombres, los apellidos, y las iniciales comunes.

El DHAP es una característica admitida en los dispositivos de seguridad del contenido de Cisco que pueden ser habilitados cuando se utiliza la validación de la aceptación del Lightweight Directory Access Protocol (LDAP). La característica DHAP no pierde de vista el número de direccionamientos receptores inválidos de un remitente dado.

Una vez que un remitente cruza un umbral administrador-definido, el remitente se juzga ser untrusted, y el correo de ese remitente se bloquea sin la generación del requisito de diseño de red (NDR) o del código de error. Usted puede configurar el umbral basado sobre la reputación del remitente. Por ejemplo, los remitentes untrusted o sospechosos pueden tener un umbral bajo DHAP, y los remitentes confiados en o reputables pueden tener un alto umbral DHAP.

Permiso DHAP

Para habilitar la característica DHAP, navegue **para enviar las directivas >** la **tabla del acceso del host (SOMBRERO) del** dispositivo de seguridad contento GUI y para seleccionar las **directivas del flujo de correo**. Elija la directiva que usted desea editar de la columna del **nombre de la directiva**.

El SOMBRERO tiene cuatro reglas de acceso básicas que se utilicen para actuar sobre las conexiones de los host remotos:

- ACCEPT (Aceptar): Se valida la conexión, y la aceptación del correo electrónico es restringida más lejos por las configuraciones del módulo de escucha. Esto incluye la tabla receptora del acceso (para los módulos de escucha públicos).

- **RECHAZO**: La conexión se valida inicialmente, solamente el cliente que las tentativas de conectar reciben un saludo 4XX o 5XX. No se valida ningún correo electrónico.

- **TCPREFUSE**: La conexión se rechaza en el nivel TCP.

- **RETRANSMISIÓN**: Se valida la conexión. La recepción para cualquier beneficiario es permitida y no obligada por la tabla receptora del acceso. La firma de las claves del dominio está disponible solamente en las directivas del flujo de correo de la retransmisión.

En la sección de los **límites del flujo de correo de la** directiva seleccionada, el hallazgo y fijó la configuración de la **prevención del ataque de recopilación de direcciones (DHAP)** fijando a los beneficiarios inválidos máximos por la hora. Usted puede también elegir personalizar los beneficiarios inválidos máximos por el código de la hora y a Max. Invalid Recipients por el texto de la hora si usted desea tan.

Usted debe relanzar esta sección para configurar DHAP para las directivas adicionales.

Asegúrese de que usted someta y confíe todos los cambios en el GUI.

> Nota: Cisco recomienda que usted utiliza un número máximo entre cinco y diez para el **número máximo de beneficiarios inválidos por la hora de una** configuración del **host remoto**.

Nota: Para la información adicional, refiera al **guía del usuario de AsyncOS** en el portal del soporte de Cisco.