Activation des fonctionnalités ESA DHAP

Contenu

Introduction

Ce document décrit comment activer la fonctionnalité Directory Harvest Attack Prevention (DHAP) sur le dispositif de sécurité de la messagerie Cisco (ESA) afin d'empêcher les attaques Directory Harvest (DHA).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ESA Cisco
- AsyncOS

Components Used

Les informations contenues dans ce document sont basées sur toutes les versions d'AsyncOS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Un DHA est une technique utilisée par les spammeurs pour localiser des adresses e-mail valides. Deux techniques principales sont utilisées pour générer les adresses que le DHA cible :

- Le spammeur crée une liste de toutes les combinaisons possibles de lettres et de chiffres, puis ajoute le nom de domaine.

- Le spammeur utilise une attaque de dictionnaire standard avec la création d'une liste qui combine les prénoms, les noms et les initiales courants.

Le protocole DHAP est une fonctionnalité prise en charge sur les dispositifs de sécurité du

contenu Cisco qui peut être activée lorsque la validation d'acceptation LDAP (Lightweight Directory Access Protocol) est utilisée. La fonctionnalité DHAP effectue le suivi du nombre d'adresses de destinataires non valides d'un expéditeur donné.

Lorsqu'un expéditeur dépasse un seuil défini par l'administrateur, il est considéré comme n'étant pas fiable et les messages de cet expéditeur sont bloqués sans spécification de conception de réseau (NDR) ni génération de code d'erreur. Vous pouvez configurer le seuil en fonction de la réputation de l'expéditeur. Par exemple, les expéditeurs non approuvés ou suspects peuvent avoir un seuil DHAP faible et les expéditeurs approuvés ou fiables peuvent avoir un seuil DHAP élevé.

Activer DHAP

Afin d'activer la fonctionnalité DHAP, accédez à **Politiques de messagerie > Table d'accès hôte (HAT)** à partir de l'interface graphique utilisateur de l'appliance de sécurité du contenu et sélectionnez **Politiques de flux de messagerie**. Sélectionnez la stratégie que vous souhaitez modifier dans la colonne **Nom de la stratégie**.

Le HAT dispose de quatre règles d'accès de base qui sont utilisées pour agir sur les connexions des hôtes distants :

- **ACCEPT (ACCEPTER):** La connexion est acceptée et l'acceptation des e-mails est limitée par les paramètres de l'écouteur. Cela inclut le tableau d'accès aux destinataires (pour les écouteurs publics).

- **REJETER** : La connexion est initialement acceptée, mais le client qui tente de se connecter reçoit un message d'accueil 4XX ou 5XX. Aucun e-mail n'est accepté.

- **TCPREFUSE** : La connexion est refusée au niveau TCP.

- **RELAIS** : La connexion est acceptée. La réception d'un destinataire est autorisée et n'est pas limitée par le tableau d'accès aux destinataires. La signature des clés de domaine est disponible uniquement sur les stratégies de flux de messages de relais.

Dans la section **Limites de flux de messages** de la stratégie sélectionnée, recherchez et définissez la configuration **Directory Harvest Attack Prevention (DHAP)** en définissant la valeur Max. Destinataires non valides par heure. Vous pouvez également choisir de personnaliser le Max. Code de destinataires par heure et max. non valides. Texte des destinataires par heure non valide si vous le souhaitez.

Vous devez répéter cette section afin de configurer le protocole DHAP pour des stratégies supplémentaires.

Assurez-vous d'envoyer et de valider toutes les modifications dans l'interface utilisateur graphique.

> **Note**: Cisco recommande d'utiliser un nombre maximal compris entre cinq et dix pour le **nombre maximal de destinataires non valides par heure à partir d'un** paramètre d'**hôte distant**.

Note: Pour plus d'informations, consultez le **Guide de l'utilisateur AsyncOS** sur le Portail d'assistance Cisco.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.