Abilitazione funzione DHCP ESA

Sommario

Introduzione

In questo documento viene descritto come abilitare la funzione Directory Harvest Attack Prevention (DHAP) su Cisco Email Security Appliance (ESA) per prevenire gli attacchi Directory Harvest (DHA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco ESA
- AsyncOS

Componenti usati

Le informazioni di questo documento si basano su tutte le versioni di AsyncOS.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Un DHA è una tecnica utilizzata dagli spammer per individuare indirizzi e-mail validi. Per generare gli indirizzi di destinazione DHA vengono utilizzate due tecniche principali:

- Lo spammer crea un elenco di tutte le possibili combinazioni di lettere e numeri, quindi aggiunge il nome di dominio.

- Lo spammer utilizza un attacco di dizionario standard con la creazione di un elenco che combina nomi, cognomi e iniziali comuni.

Il protocollo DHCP è una funzionalità supportata nelle appliance Cisco Content Security che può essere abilitata quando si utilizza la convalida di accettazione LDAP (Lightweight Directory Access Protocol). La funzionalità DHCP consente di tenere traccia del numero di indirizzi di destinatari non validi provenienti da un determinato mittente.

Quando un mittente supera una soglia definita dall'amministratore, viene considerato non attendibile e la posta proveniente da tale mittente viene bloccata senza alcun requisito di progettazione della rete o generazione di codice di errore. È possibile configurare la soglia in base alla reputazione del mittente. Ad esempio, i mittenti non attendibili o sospetti possono avere una soglia DHCP bassa e i mittenti attendibili o attendibili possono avere una soglia DHCP alta.

Abilita DHCP

Per abilitare la funzione DHCP, selezionare **Mail Policies > Host Access Table (HAT)** dalla GUI di Content Security Appliance e selezionare **Mail Flow Policies** (Policy di flusso di posta). Scegliere il criterio che si desidera modificare dalla colonna **Nome criterio**.

HAT dispone di quattro regole di accesso di base che vengono utilizzate per agire sulle connessioni dagli host remoti:

- **ACCETTA**: La connessione viene accettata e l'accettazione della posta elettronica viene ulteriormente limitata dalle impostazioni del listener. inclusa la tabella Accesso destinatario (per i listener pubblici).
- **RIFIUTA**: La connessione è inizialmente accettata, ma il client che tenta di connettersi riceve un messaggio di saluto 4XX o 5XX. Nessun messaggio di posta elettronica accettato.
- **TCPREFUSE**: Connessione rifiutata a livello TCP.
- **RELÈ**: La connessione è accettata. La ricezione per qualsiasi destinatario è consentita e non è vincolata dalla tabella Accesso destinatario. La firma delle chiavi di dominio è disponibile solo nei criteri del flusso di posta di inoltro.

Nella sezione **Limiti flusso posta** del criterio selezionato, individuare e impostare la configurazione **DHCP (Directory Harvest Attack Prevention)** impostando il valore Max. Destinatari non validi all'ora. È inoltre possibile personalizzare il valore Max. Il codice per ora dei destinatari non è valido e il valore massimo. Testo Destinatari non validi all'ora, se lo si desidera.

È necessario ripetere questa sezione per configurare il protocollo DHCP per altri criteri.

Accertarsi di inviare ed eseguire il commit di tutte le modifiche nella GUI.

> **Nota:** Cisco consiglia di utilizzare un numero massimo compreso tra cinque e dieci per il **numero massimo di destinatari non validi all'ora da un'**impostazione di **host remoto**.

> **Nota:** Per ulteriori informazioni, fare riferimento alla **Guida per l'utente di AsyncOS** sul portale di supporto Cisco.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).