Que « le message d'avertissement détecté par attaque potentielle de récolte de répertoire » signifie-t-il ?

Contenu

Introduction

Ce document décrit le message d'erreur « de répertoire d'attaque potentielle de récolte » comme reçu sur l'appliance de sécurité du courrier électronique de Cisco (ESA).

Que « le message d'avertissement détecté par attaque potentielle de récolte de répertoire » signifie-t-il ?

Les administrateurs pour l'ESA ont reçu le message d'avertissement suivant de la prévention d'attaque de récolte de répertoire (DHAP) :

```
The Warning message is:

Potential Directory Harvest Attack detected. See the system mail logs for more
information about this attack.

Version: 8.0.1-023
Serial Number: XXBAD1112DYY-008X011
Timestamp: 22 Sep 2014 21:21:32 -0600
```

Ces alertes sont considérées informationnelles et vous ne devriez pas devoir ne prendre aucune mesure. Un serveur de messagerie extérieur a tenté trop de destinataires non valides et a déclenché l'alerte DHAP (prévention d'attaque de récolte de répertoire). L'ESA agit en tant que configuré basé sur la configuration de politique de messagerie.

C'est le nombre maximal de destinataires non valides par heure où l'auditeur recevra d'un serveur distant. Ce seuil représente le nombre total de rejets de serveur de rejets de RAT et d'appel-en avant de SMTP combinés avec le nombre total de messages aux destinataires non valides de LDAP abandonnés dans la conversation de SMTP ou rebondis dans la file d'attente de travail (comme configuré dans le LDAP recevez les configurations sur l'auditeur associé). Pour plus d'informations sur configurer DHAP pour le LDAP recevez les requêtes, voient que le « LDAP

questionne » le chapitre du guide utilisateur de sécurité du courrier électronique.

Vous pouvez ajuster votre profil vigilant avec l'**alertconfig** pour filtrer ces derniers si vous ne souhaitez pas recevoir ces alertes :

```
myesa.local> alertconfig

Sending alerts to:
robert@domain.com
Class: All - Severities: All

Initial number of seconds to wait before sending a duplicate alert: 300
Maximum number of seconds to wait before sending a duplicate alert: 3600
Maximum number of alerts stored in the system are: 50

Alerts will be sent using the system-default From Address.

Cisco IronPort AutoSupport: Enabled
You will receive a copy of the weekly AutoSupport reports.

Choose the operation you want to perform:
- NEW - Add a new email address to send alerts.
- EDIT - Modify alert subscription for an email address.
- DELETE - Remove an email address.
- CLEAR - Remove all email addresses (disable alerts).
- SETUP - Configure alert settings.
- FROM - Configure the From Address of alert emails.
[]> edit

Please select the email address to edit.
1. robert@domain.com (all)
[]> 1

Choose the Alert Class to modify for "robert@domain.com".
Press Enter to return to alertconfig.
1. All - Severities: All
2. System - Severities: All
3. Hardware - Severities: All
4. Updater - Severities: All
5. Outbreak Filters - Severities: All
6. Anti-Virus - Severities: All
7. Anti-Spam - Severities: All
8. Directory Harvest Attack Prevention - Severities: All
```

Ou de l'**administration système** GUI **> alerte >** ***adresse réceptive*** et modifie la sévérité reçue, ou l'alerte en sa totalité.

GUI

Pour visualiser vos paramètres de configuration DHAP du GUI, clic par des **stratégies de messagerie > stratégies >** ***clic de*** **flux de courrier le nom de stratégie** ***à éditer, ou*** **paramètres de stratégie par défaut >** et à apporter des modifications aux **limites de flux de courrier/à la** section de la **prévention d'attaque récolte de répertoire (DHAP)** comme nécessaire :

Soumettez et **commettez** vos modifications au GUI.

CLI

Pour visualiser vos paramètres de configuration DHAP du CLI, le **listenerconfig d'**utilisation **> éditent** (*choisissant le nombre de l'auditeur pour éditer*) **> des hostaccess > par défaut** pour éditer les configurations DHAP :

```
Default Policy Parameters
==========================
Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Maximum Number of Recipients per Envelope Sender: Disabled
Use SenderBase for Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces: No

There are currently 5 policies defined.
There are currently 8 sender groups.

Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- RESET - Remove senders and set policies to system default.
[]> default

Enter the default maximum message size. Add a trailing k for kilobytes, M for
megabytes, or no letter for bytes.
[10M]>

Enter the maximum number of concurrent connections allowed from a single
IP address.
[10]>

Enter the maximum number of messages per connection.
[10]>

Enter the maximum number of recipients per message.
[50]>

Do you want to override the hostname in the SMTP banner? [N]>
```

```
Would you like to specify a custom SMTP acceptance response? [N]>

Would you like to specify a custom SMTP rejection response? [N]>

Do you want to enable rate limiting per host? [N]>

Do you want to enable rate limiting per envelope sender? [N]>

Do you want to enable Directory Harvest Attack Prevention per host? [Y]>

Enter the maximum number of invalid recipients per hour from a remote host.
[25]>

Select an action to apply when a recipient is rejected due to DHAP:
1. Drop
2. Code
[1]>

Would you like to specify a custom SMTP DHAP response? [Y]>

Enter the SMTP code to use in the response. 550 is the standard code.
[550]>

Enter your custom SMTP response. Press Enter on a blank line to finish.

Would you like to use SenderBase for flow control by default? [Y]>

Would you like to enable anti-spam scanning? [Y]>

Would you like to enable anti-virus scanning? [Y]>

Do you want to allow encrypted TLS connections?
1. No
2. Preferred
3. Required
4. Preferred - Verify
5. Required - Verify
[1]>

Would you like to enable DKIM/DomainKeys signing? [N]>

Would you like to enable DKIM verification? [N]>

Would you like to change SPF/SIDF settings? [N]>

Would you like to enable DMARC verification? [N]>

Would you like to enable envelope sender verification? [N]>

Would you like to enable use of the domain exception table? [N]>

Do you wish to accept untagged bounces? [N]>
```

Si vous faites n'importe quelles mises à jour ou changez, revenez à la demande principale CLI et **commettez** toutes les modifications.

Informations connexes

- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- Support et documentation techniques - Cisco Systems