Les emails chiffrés par S/MIME perdent leur contenu après que des balises ESA/CES

Contenu

Introduction

Ce document décrit pourquoi les emails sécurisés/MIMES (S/MIME) reçus dans la boîte de réception de destinataires ne contient aucun contenu après avoir traversé l'appliance de sécurité du courrier électronique (ESA) ou la sécurité du courrier électronique de nuage (CES).

Problème : Les emails perdent leur contenu après que les balises ESA/CES.

Une organisation a configuré ses emails à signer ou chiffré par des Certificats S/MIME et après avoir été envoyé par un périphérique de Cisco ESA/CES, l'email semble l'avoir perdu est satisfait quand il arrive dans la boîte de réception de destinataires d'extrémité. Ce comportement se produit généralement quand l'ESA/CES est configuré pour modifier le contenu de l'email, la modification typique de l'ESA/CES est étiquetage de déni de responsabilité.

Quand un email est signé ou chiffré avec S/MIME, tout le contenu de corps est haché pour protéger son intégrité. Quand tous les serveurs de messagerie trifouillent le contenu en modifiant le corps, d'informations parasites les correspondances plus cela qui a été signé/chiffré et cause consécutivement le contenu de corps d'être perdu.

En outre, des emails qui sont chiffrés avec la signature « opaque » S/MIME ou S/MIME d'utilisation (c.-à-d. des fichiers p7m) ne peuvent être automatiquement identifiés par le logiciel S/MIME sur l'extrémité réceptrice s'ils sont modifiés. Dans le cas d'un email p7m S/MIME, le contenu de l'email, y compris des connexions, est contenu dans le fichier de .p7m. Si la structure est réorganisée quand l'ESA/CES ajoute le déni de responsabilité emboutissant, ce fichier de .p7m peut plus n'être dans un endroit où le logiciel de messagerie qui manipule le S/MIME peut correctement le comprendre.

Typiquement des emails qui sont signés ou chiffrés par S/MIME ne devraient pas être modifiés du tout. Quand l'ESA/CES est la passerelle configurée à signer/chiffre un email, ceci devrait être fait après que n'importe quelle modification de l'email soit exigée, et généralement quand l'ESA/CES est le dernier saut qui manipule l'email avant de l'envoyer au serveur de messagerie du destinataire.

Solution

Afin d'éviter la manipulation ESA/CES ou la modification des emails entrants de l'Internet qui sont S/MIME chiffrés, configurez un filtre de message pour localiser l'email pour ajouter une X-**en-tête** et pour ignorer tous filtres restants de message, suivis de créer un filtre satisfait pour localiser cette X-en-tête et pour ignorer les filtres satisfaits restants qui peuvent modifier le contenu de corps/connexion.

> **Attention** : En fonctionnant avec le saut-filters() ; les filtres satisfaits restants d'action ou de saut (mesure finale) la commande des filtres est très essentiel. L'établissement d'un filtre de saut dans une commande incorrecte peut permettre au message pour ignorer quelques filtres fortuits.

Ceci inclut mais non limité à :

- Les réécritures de Filtrage URL, defang et des réécritures sécurisées de proxy.
- Déni de responsabilité étiquetant sur l'email.
- Envoyez le balayage de corps et le remplacez.

> Remarque: Pour obtenir l'accès à la ligne de commande de solution de CES, référez-vous s'il vous plaît au guide CLI de CES.

Afin de configurer un filtre de message, procédure de connexion à l'ESA/CES du CLI :

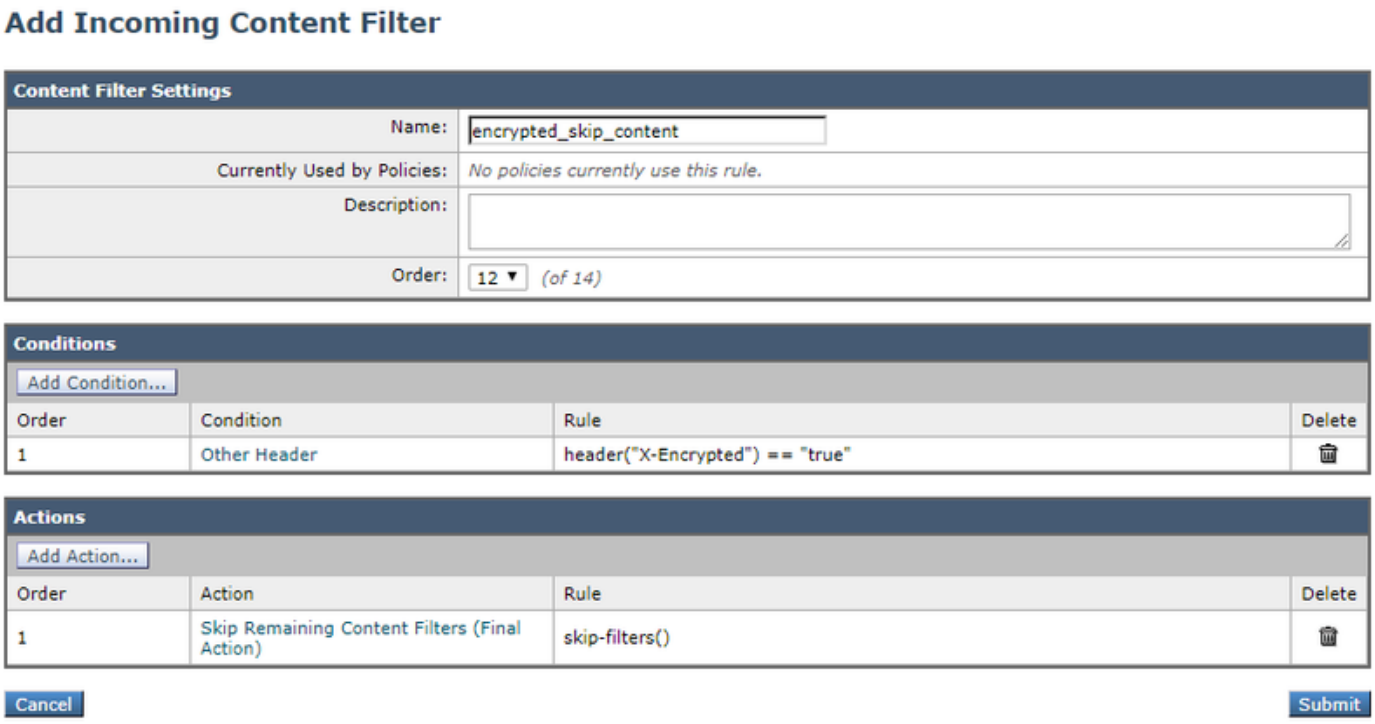
```
C680.esa.lab> filters


Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> new

Enter filter script. Enter '.' on its own line to end.
encrypted_skip:
if (encrypted)
{
insert-header("X-Encrypted", "true");
skip-filters();
}
.
1 filters added.
```

> Remarque: L'attaque de virus de Cisco filtre quand le positionnement avec la **modification de message** entraîne également le S/MIME signant/informations parasites de cryptage pour échouer. En cas la stratégie de messagerie a des filtres d'attaque de virus activés avec la modification de message, elle est recommandée de désactiver la modification de message sur la stratégie assortie de messagerie ou d'ignorer l'épidémie filtrant aussi bien avec une action de filtre de message de **saut-outbreakcheck() ;.**

Après que le filtre de message soit configuré pour étiqueter les emails chiffrés avec une X-en-tête, pour créer un filtre satisfait pour localiser cette en-tête et pour appliquer l'action satisfaite restante de filtre de saut.



Configurez ce filtre satisfait dans vos stratégies existantes de messagerie entrante où les emails chiffrés devraient ignorer les filtres satisfaits qui restent.

Informations connexes

- Comment vérifier des messages envoyés avec S/MIME envoyant le profil sur l'ESA
- Comment vérifier des messages reçus avec S/MIME sur l'ESA
- Support et documentation techniques - Cisco Systems
- Appliance de sécurité du courrier électronique de Cisco - Guides utilisateurs