Os email cifrados S/MIME perdem seu índice após etiquetas ESA/CES

Índice

Introdução

Este original descreve porque os email seguros/Multipurpose Internet Mail Extension (S/MIME) recebidos na caixa de entrada dos receptores não contêm nenhum índice após a passagem com a Segurança do email da ferramenta de segurança (ESA) ou da nuvem do email (CES).

Problema: Os email perdem seu índice após as etiquetas ESA/CES.

Uma organização configurou seus email a ser assinados ou cifrado por Certificados S/MIME e após a emissão através de um dispositivo de Cisco ESA/CES, o email parece tê-lo perdido é satisfeito quando chega na caixa de entrada dos receptores da extremidade. Este comportamento ocorre geralmente quando o ESA/CES é configurado para alterar os índices do email, a alteração típica do ESA/CES é colocação de etiquetas da negação.

Quando um email é assinado ou cifrado com S/MIME, todo o índice do corpo está picado para proteger sua integridade. Quando todos os server do correio alteram o índice alterando o corpo, da mistura os fósforos já não isso que foi assinado/cifrado e fazem com por sua vez que o índice do corpo esteja perdido.

Além disso, os email que são cifrados com assinatura “opaca” S/MIME ou S/MIME do uso (isto é arquivos p7m) não podem automaticamente ser reconhecidos pelo software S/MIME na extremidade de recepção se são alterados. No caso de um email p7m S/MIME, os índices do email, incluindo acessórios, são contidos dentro do arquivo de .p7m. Se a estrutura é reorganizada quando o ESA/CES adiciona a negação que carimba, este arquivo de .p7m pode já não ser em um lugar onde o software M.U.A. que segura o S/MIME possa corretamente o compreender.

Tipicamente os email que são assinados ou cifrados por S/MIME não devem ser alterados de todo. Quando o ESA/CES é o gateway configurado para assinar/cifra um email, isto deve ser feito depois que toda a alteração do email é exigida, e geralmente quando o ESA/CES for o último salto que segura o email antes do enviar ao mail server do receptor.

Solução

A fim evitar a manipulação ESA/CES ou a alteração dos email entrantes do Internet que são

S/MIME cifrados, configurar um filtro da mensagem para encontrar o email para adicionar um X-**encabeçamento** e para saltar todos os filtros restantes da mensagem, seguidos criando um filtro satisfeito para encontrar este X-encabeçamento e para saltar os filtros satisfeitos restantes que podem alterar os índices do corpo/acessório.

> Cuidado: Ao trabalhar com faixa clara-filters(); os filtros satisfeitos restantes da ação ou da faixa clara (ação final) a ordem dos filtros são muito críticos. Ajustar um filtro da faixa clara em uma ordem incorreta pode permitir que a mensagem salte alguns filtros sem intenção.

Isto inclui mas não limitado a:

- As reescritas da Filtragem URL, defang e reescritas seguras do proxy.
- Negação que etiqueta no email.
- Envie por correio eletrónico a varredura do corpo e substitua-a.

> Nota: Para obter o acesso à linha de comando da solução CES, refira por favor o guia CES CLI.

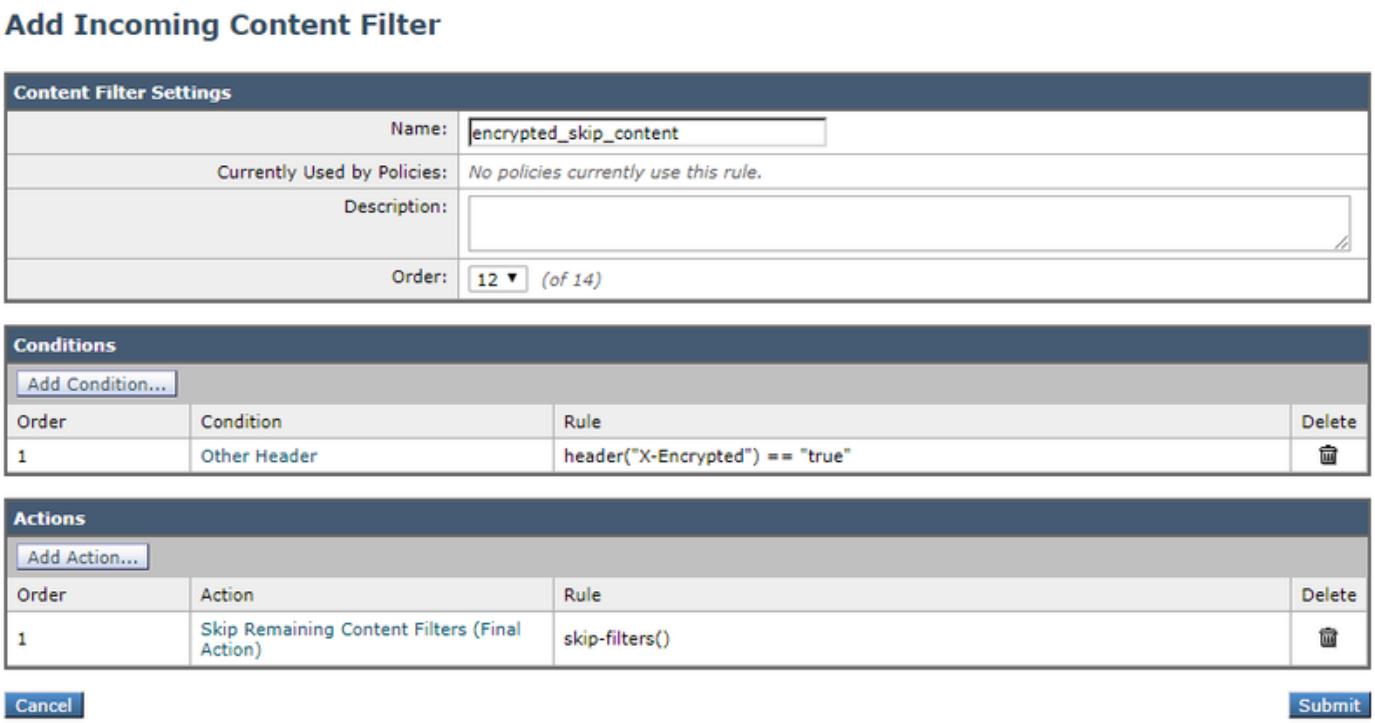
A fim configurar um filtro da mensagem, entre ao ESA/CES do CLI:

```
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.
```

> Nota: Filtros da manifestação do vírus de Cisco quando o grupo com **alteração da mensagem** igualmente causar o S/MIME que assina/mistura da criptografia para falhar. No evento a política do correio tem os filtros da manifestação do vírus permitidos com alteração da mensagem, recomenda-se desabilitar a alteração da mensagem na política de harmonização do correio ou saltar a manifestação que filtra também com uma ação do filtro da mensagem da **faixa clara-outbreakcheck();**.

Depois que o filtro da mensagem é configurado para etiquetar email cifrados com um X-

encabeçamento, para criar um filtro satisfeito para encontrar este encabeçamento e para aplicar a ação do filtro satisfeita restante da faixa clara.



Configurar este filtro satisfeito em suas políticas existentes do correio recebido onde os email cifrados devem saltar os filtros satisfeitos que permanecem.

Informações Relacionadas

- Como verificar as mensagens enviadas com o S/MIME que envia o perfil no ESA
- Como verificar as mensagens recebidas com o S/MIME no ESA
- Suporte Técnico e Documentação - Cisco Systems
- Cisco envia por correio eletrónico a ferramenta de segurança - Guias do Usuário