S/MIME-versleutelde e-mails hun inhoud verliezen na ESR/CES-tags

Inhoud

Inleiding

In dit document wordt beschreven waarom beveiligde/multifunctionele Internet Mail Uitbreidingen (S/MIME) e-mails die in ontvangers zijn ontvangen, geen inhoud bevatten nadat ze via de e-mail security applicatie (ESA) of Cloud Email Security (CES) zijn verzonden.

Probleem: E-mails verliezen hun content na de ESA/CES-tags.

Een organisatie heeft haar e-mails ingesteld die door S/MIME-certificaten moeten worden getekend of versleuteld en na door een Cisco ESA/CES-apparaat te zijn verstuurd, lijkt de e-mail de inhoud te hebben verloren wanneer deze in het uiteinde wordt ontvangen in het inbox. Dit gedrag doet zich doorgaans voor wanneer de ESA/CES is ingesteld om de inhoud van de e-mail aan te passen. De typische wijziging van de ESA/CES is het markeren van de gegevens.

Wanneer een e-mail is getekend of versleuteld met S/MIME, wordt alle inhoud van het lichaam beschadigd om de integriteit ervan te beschermen. Wanneer mailservers met de inhoud knoeien door het lichaam te wijzigen, komt de hash niet langer overeen met de inhoud die getekend/gecodeerd is en zorgt hij er op zijn beurt voor dat de inhoud van het lichaam verloren gaat.

Bovendien kunnen e-mails die versleuteld zijn met S/MIME of die 'ondoorzichtig' S/MIME-gebaren gebruiken (d.w.z. p7m-bestanden), niet automatisch door S/MIME-software worden herkend als ze worden aangepast. Bij een p7m S/MIME-e-mail bevat de inhoud van de e-mail, met inbegrip van de bijlagen, het .p7m-bestand. Als de structuur wordt gereorganiseerd wanneer de ESA/CES de disclaimer-stempeling toevoegt, is dit .p7m-bestand mogelijk niet langer op een plaats waar de MUA-software die de S/MIME verwerkt het naar behoren kan begrijpen.

Meestal worden e-mails die door S/MIME zijn ondertekend of versleuteld, helemaal niet gewijzigd. Wanneer de ESA/CES de toegangspoort is om een e-mail te ondertekenen/te versleutelen, dient dit te gebeuren nadat de e-mail moet worden gewijzigd en doorgaans wanneer de ESA/CES de laatste hop is die de e-mail verwerkt voordat deze naar de mailserver van de ontvanger wordt verzonden.

Oplossing

Om te voorkomen dat de ESA/CES-manipulatie of wijziging optreedt van binnenkomende e-mails

van het internet die S/MIME-versleuteld zijn, moet u een bericht-filter configureren om een **X-header** toe te voegen en eventuele resterende berichtfilters te overslaan, gevolgd door een filter te maken om deze X-header te vinden en de resterende inhoudfilters te overslaan die de inhoud van het bericht of de bijlage kunnen wijzigen.

> **Voorzichtig:** Bij het werken met skip-filters(); Handeling of Niet resterende Filters van de Inhoud (Eindactie) de volgorde van de filters is zeer kritiek. Wanneer u een skip-filter in een incorrecte volgorde instelt, kan het bericht bepaalde filters onbedoeld overslaan.

Dit omvat, maar niet beperkt tot:

- URL-filtering herschrijft, zowel verdediging als beveiligde proxy herschrijft.
- Disclaimer die op de e-mail tagt.
- E-maillichaam scannen en vervangen.

> Opmerking: Raadpleeg de CES CLI Guide om toegang te krijgen tot de CES Solution-opdrachtregel.

Om een berichtfilter te configureren logt u in op de ESA/CES van de CLI:

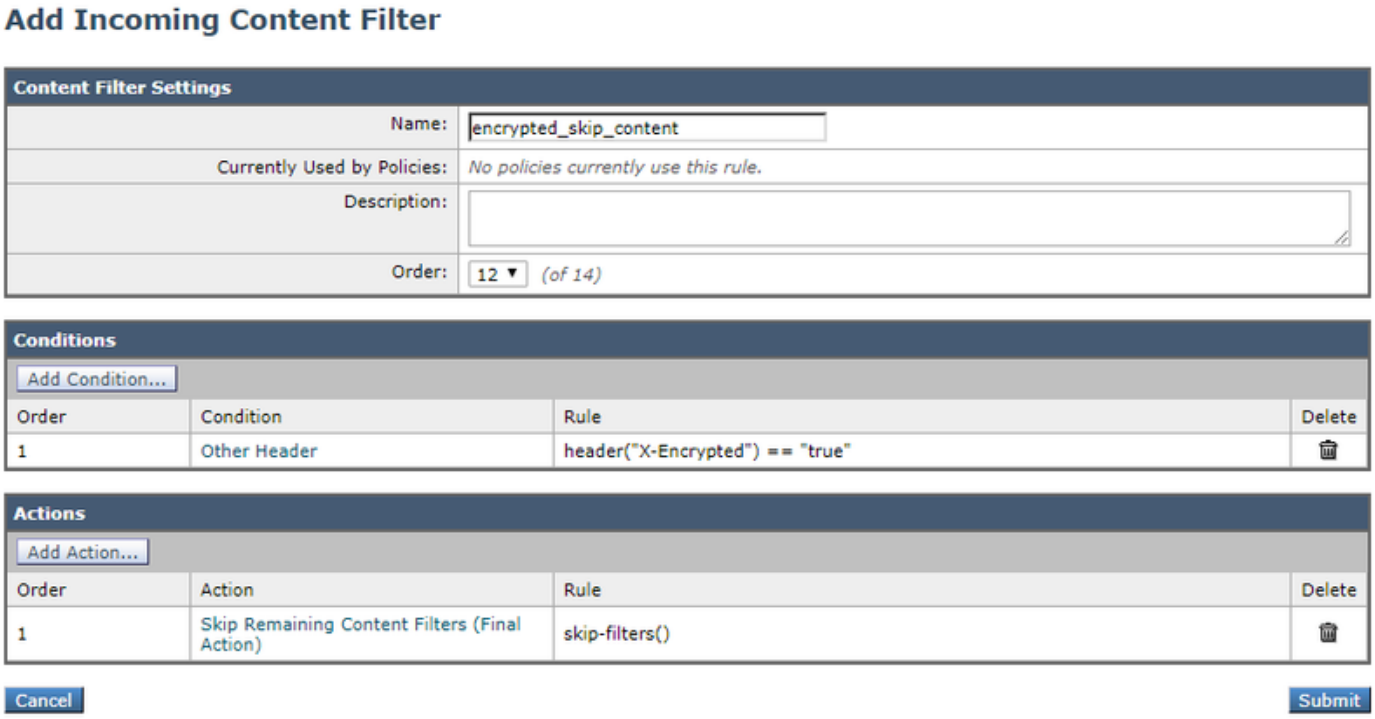
```
C680.esa.lab> filters


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.
```

> Opmerking: Cisco Virus Outbreak Filters wanneer deze ingesteld wordt met **Berichtwijziging** zorgt er ook voor dat de S/MIME-teken/encryptie-hash niet werkt. Als het postbeleid Filters van het virus heeft die zijn ingeschakeld met de wijziging van het bericht, wordt aanbevolen om berichtwijziging uit te schakelen in het postbeleid of het filteren van uitbraken van het e-mailadres of om een berichtfilteractie van **skip-outbreakcheck()** uit te schakelen**; .**

Nadat het berichtfilter is ingesteld om versleutelde e-mails met een X-Kop te taggen, maakt u een inhoudfilter om deze kop te plaatsen en de overgebleven contentfilteractie toe te passen.



Configuratie van deze inhoudsfilter in uw bestaand inkomende e-mailbeleid waar de gecodeerde e-mails de inhoudfilters zouden moeten overslaan die blijven.

Gerelateerde informatie

- Bestaan van berichten die worden verzonden met S/MIME-verkeersprofiel op ESA
- Hoe de bij S/MIME ontvangen berichten op ESA worden geverifieerd
- Technische ondersteuning en documentatie – Cisco Systems
- Cisco e-mail security applicatie - gebruikershandleidingen