Échec du dépannage de l'ouverture des e-mails chiffrés traités par Mimecast Secure Email Gateway

Contenu

Introduction

Ce document décrit un problème avec les e-mails chiffrés de Cisco Secure Email Encryption Service (anciennement Cisco Registered Envelope Service) si l'entité qui reçoit les e-mails a une passerelle de messagerie sécurisée Mimecast et que les réécritures d'URL sont activées.

Problème

Deux comportements distincts ont été observés sur le terrain en ce qui concerne l'intégration de Mimecast et de Cisco Secure Email Encryption.

- Mimecast remplace la barre oblique inverse par une barre oblique inverse, ce qui entraîne un échec de redirection du navigateur.
- Mimecast réécrit l'URL dans la pièce jointe et corrompt la charge utile.

Problème de redirection du navigateur

Description

Mimecast Secure Email Gateway remplace la barre oblique inverse par une barre oblique inverse dans la pièce jointe securedoc.html, ce qui corrompt alors la charge utile et empêche les utilisateurs finaux d'ouvrir les messages.

Symptômes

Les symptômes généraux comprennent les utilisateurs finaux qui ne peuvent pas entrer leurs mots de passe ou dont le champ de mot de passe produit des erreurs.

Identification du problème

1. Demandez aux utilisateurs finaux concernés de partager le **fichier securedoc.html**

2. Ouvrez le fichier **securedoc.html** dans l'éditeur de texte de votre choix (par exemple, Notepad++) ou partagez-le avec le centre d'assistance technique Cisco et recherchez la chaîne : **RedirectionNavigateur**

3. Vérifiez l'URL complète avec **BrowserRedirect** et vérifiez s'il y a une barre oblique arrière ou avant à la fin.

a. URL correcte (se termine par une barre oblique) - java.sun.com/webapps/getjava/**BrowserRedirect**

b. URL problématique (se termine par une barre oblique) - java.sun.com/webapps/getjava/**BrowserRedirect/**

4. Une URL incorrecte se termine par une barre oblique et nous permet de confirmer le comportement problématique.

Solution

1. Une mise à jour du moteur de cryptage (PXE) a été publiée et comprend un correctif qui résout le problème. Exécutez **updatenow** force à partir de l'interface de ligne de commande pour déclencher la mise à jour.

```
(Machine esa.example.com)> updatenow force

Success - Force update for all components requested
```

2. Une fois la mise à jour démarrée, vous pouvez utiliser la commande **encryptionstatus** pour confirmer que la mise à jour a été appliquée.

```
(Machine esa.example.com)> encryptionstatus

Component Version Last Updated
PXE Engine 8.1.5.007 29 Jul 2022 16:58 (GMT +00:00)
Domain Mappings File 1.0.0 Never updated
```

3. En cas de succès, le résultat du moteur PXE indique la date et l'heure actuelles.

```
(Machine esa.example.com)> encryptionstatus

Component Version Last Updated
PXE Engine 8.1.5.007 29 Jul 2022 16:58 (GMT +00:00)
Domain Mappings File 1.0.0 Never updated
```

Problème de réécriture d'URL

Description

La passerelle de messagerie sécurisée Mimecast réécrit les URL dans la pièce jointe **securedoc.html**, ce qui corrompt alors la charge utile et empêche les utilisateurs finaux d'ouvrir des messages.

Symptômes

Les symptômes généraux comprennent les utilisateurs finaux qui ne peuvent pas entrer leurs mots de passe ou dont le champ de mot de passe produit des erreurs.

Identification du problème

1. Demandez aux utilisateurs finaux concernés de partager le **fichier securedoc.html**

2. Ouvrez le fichier **securedoc.html** dans l'éditeur de texte de votre choix (par exemple, Notepad++) ou partagez-le avec le centre d'assistance technique Cisco et recherchez la chaîne : **protect-us.mimecast.com**

3. Vérifiez les URL réécrites et reportez-vous à l'image pour une comparaison avant et après.

B	C
Cisco CRES	**Mimecast**
https://res.cisco.com:443">https://res.cisco.com:443	https://protect-us.mimecast.com/s/qe5vCjRJ6RUj1mRzztRupc2?domain=res.cisco.com
https://res.cisco.com:443/websafe/help?topic=AddrNotShown',{'localeUI':getLocale()})	https://protect-us.mimecast.com/s/fQ-lCkRMXRUn3B5DDIQIC_L?domain=res.cisco.com%27:getLocale()%7d
https://res.cisco.com:443/websafe/help?topic=AddrNotShown'	https://protect-us.mimecast.com/s/K-wsClY6EYioqEXWWtq8IgM?domain=res.cisco.com'
https://res.cisco.com:443/websafe/pswdForgot.action'	https://protect-us.mimecast.com/s/19AmCmZXNZf5LlWVVCQgK3j?domain=res.cisco.com
https://res.cisco.com:443/websafe/pswdForgot.action	https://protect-us.mimecast.com/s/19AmCmZXNZf5LlWVVCQgK3j?domain=res.cisco.com
https://res.cisco.com/keyserver/Logout	https://protect-us.mimecast.com/s/cJy3Cn5J65fGpDm44iEFCsD?domain=res.cisco.com
https://res.cisco.com:443/keyserver/Logout	https://protect-us.mimecast.com/s/cJy3Cn5J65fGpDm44iEFCsD?domain=res.cisco.com
https://res.cisco.com:443	https://protect-us.mimecast.com/s/qe5vCjRJ6RUj1mRzztRupc2?domain=res.cisco.com
https://res.cisco.com:443/websafe/help?topic=AddrNotShown	https://protect-us.mimecast.com/s/K-wsClY6EYioqEXWWtq8IgM?domain=res.cisco.com'
https://res.cisco.com:443/keyserver/keyserver	https://protect-us.mimecast.com/s/8FnrCpYVLYizEoAggFkH5wE?domain=res.cisco.com

4. Lorsque la pièce jointe securedoc.html est envoyée via la passerelle de messagerie sécurisée Mimecast, les URL référencées sont réécrites de manière incorrecte, ce qui entraîne la rupture de la syntaxe HTML. De ce fait, les utilisateurs finaux ne peuvent pas ouvrir les e-mails chiffrés.

Exemple :

https://res.cisco.com:443/websafe/help?topic=AddrNotShown',**{'localeUI':getLocale()})** est réécrit dans https://protect-us.mimecast.com/s/fQ-lCkRMXRUn3B5DDIQIC_L?domain=res.cisco.com**':getLocale()})**. Comme vous pouvez le voir, une fois les URL réécrites, le champ **localeUI** est supprimé.

Solutions

1. Transférez l'e-mail en question à mobile@res.cisco.com. Une fois reçu, l'utilisateur final peut cliquer sur le lien et déchiffrer l'e-mail.

ou

2. Activez la fonction Easy Open. Les e-mails chiffrés sont envoyés aux destinataires avec un lien d'affichage dans le corps de l'e-mail. Les utilisateurs finaux peuvent alors cliquer sur le lien et déchiffrer l'e-mail.

ou

3. Ignorez le domaine de l'expéditeur res.cisco.com sur la passerelle de messagerie sécurisée Mimecast.

Additional Information

Documentation de Cisco Secure Email Gateway

- notes de version
- Guide de l'utilisateur
- Guide de référence CLI

- Guides de programmation API pour Cisco Secure Email Gateway
- Open Source utilisé dans Cisco Secure Email Gateway
- Guide d'installation de l'appliance virtuelle de sécurité du contenu Cisco (inclut vESA)

Documentation sur Secure Email Cloud Gateway

- notes de version
- Guide de l’utilisateur

Documentation de Cisco Secure Email and Web Manager

- Notes de version et matrice de compatibilité
- Guide de l’utilisateur
- Guides de programmation API pour Cisco Secure Email and Web Manager
- Guide d'installation de l'appliance virtuelle de sécurité du contenu Cisco (inclut vSMA)

Documentation produit Cisco Secure

- Architecture d'attribution de noms Cisco Secure