Resolución de problemas Fallo al abrir correos electrónicos cifrados procesados por Mimecast Secure Email Gateway

Contenido

Introducción

Este documento describe un problema con los correos electrónicos cifrados del Servicio de cifrado de correo electrónico seguro de Cisco (anteriormente, Servicio de sobres registrados de Cisco) si la entidad que recibe los correos electrónicos tiene un gateway de correo electrónico seguro Mimecast y las reescrituras de URL están habilitadas.

Problema

Se han observado dos comportamientos independientes en este campo con respecto a la integración de Mimecast y Cisco Secure Email Encryption.

- Mimecast cambia la barra diagonal inversa a una barra diagonal, lo que da lugar a una falla de redirección del navegador.
- Mimecast reescribe la URL en el adjunto y corrompe la carga.

Problema de redirección del navegador

Descripción

Mimecast Secure Email Gateway cambia la barra diagonal inversa a una barra diagonal en el archivo adjunto securedoc.html, lo que corrompe la carga y hace que los usuarios finales no puedan abrir los mensajes.

Síntomas

Los síntomas generales incluyen a los usuarios finales que no pueden introducir sus contraseñas o que el campo de contraseña produce errores.

Identificar el problema

1. Solicite a los usuarios finales afectados que compartan el archivo **securedoc.html**

2. Abra el archivo **securedoc.html** en el editor de texto que elija (por ejemplo, Notepad++) o compártalo con Cisco TAC y busque la cadena: **BrowserRedirect**

3. Revise la URL completa con **BrowserRedirect** y confirme si hay una barra diagonal o inversa al final.

a. URL correcta (termina con barra diagonal inversa) - java.sun.com/webapps/getjava/**BrowserRedirect**

b. URL problemática (termina con barra diagonal): java.sun.com/webapps/getjava/**BrowserRedirect/**

4. Una URL incorrecta termina con una barra diagonal y nos permite confirmar el comportamiento problemático.

Solución

1. Se ha lanzado una actualización del motor de cifrado (PXE) que incluye una solución que resuelve el problema. Ejecute **update**now force desde la CLI para activar la actualización.

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

Success - Force update for all components requested
```

2. Una vez iniciada una actualización, puede utilizar el comando **encryptionstatus** para confirmar que se ha aplicado la actualización.

```
(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. Si se ejecuta correctamente, la salida del motor PXE muestra la fecha y la hora actuales.


```
(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
```


Problema de reescritura de URL

Descripción

Mimecast Secure Email Gateway reescribe las URL en el archivo adjunto **securedoc.html**, lo que corrompe la carga y hace que los usuarios finales no puedan abrir los mensajes.

Síntomas

Los síntomas generales incluyen a los usuarios finales que no pueden introducir sus contraseñas o que el campo de contraseña produce errores.

Identificar el problema

1. Solicite a los usuarios finales afectados que compartan el archivo **securedoc.html**

2. Abra el archivo **securedoc.html** en el editor de texto que elija (por ejemplo, Notepad++) o compártalo con Cisco TAC y busque la cadena: **protect-us.mimecast.com**

3. Revise las URL reescritas y consulte la imagen para ver una comparación antes y después.

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/19AmCmZXNZf5LIWVVCQgK3j?domain=res.cisco.com
https://res.cisco.com:443/websafe/pswdForgot.action	https://protect-us.mimecast.com/s/19AmCmZXNZf5LIWVVCQgK3j?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. Cuando el adjunto securedoc.html se envía a través de Mimecast Secure Email Gateway, las URL referenciadas se reescriben incorrectamente, lo que hace que la sintaxis HTML se rompa. Debido a esto, los usuarios finales no pueden abrir los correos cifrados.

Por ejemplo:

https://res.cisco.com:443/websafe/help?topic=AddrNotShown',**{'localeUI':getLocale()})** se reescribe en https://protect-us.mimecast.com/s/fQ-lCkRMXRUn3B5DDIQIC_L?domain=res.cisco.com**':getLocale()})**. Como puede ver, después de reescribir las URL, se elimina el campo **localeUI**.

Soluciones

1. Reenvíe el correo electrónico en cuestión a mobile@res.cisco.com. Una vez recibidos, los usuarios finales podrían hacer clic en el enlace y descifrar correctamente el correo electrónico.

or

2. Active la función de apertura sencilla. Los correos electrónicos cifrados se enviarían a los destinatarios con un enlace de visualización en el cuerpo del correo electrónico. Los usuarios finales podrían hacer clic en el enlace y descifrar el correo electrónico.

or

3. Omita el dominio del remitente de res.cisco.com en Mimecast Secure Email Gateway.

Additional Information

Documentación de Cisco Secure Email Gateway

- Release Notes
- Guía del usuario
- Guía de referencia de CLI
- Guías de programación de API para Cisco Secure Email Gateway
- Código abierto utilizado en Cisco Secure Email Gateway

- Guía de instalación del appliance virtual de seguridad de contenido de Cisco(incluye vESA)

Documentación de Secure Email Cloud Gateway

- Release Notes
- Guía del usuario

Documentación de Cisco Secure Email and Web Manager

- Notas de la versión y matriz de compatibilidad
- Guía del usuario
- Guías de programación de API para Cisco Secure Email y Web Manager
- Guía de instalación del appliance virtual de seguridad de contenido de Cisco(incluye vSMA)

Documentación del producto Cisco Secure

- Arquitectura de nomenclatura de la cartera Cisco Secure