Risoluzione dei problemi: impossibile aprire i messaggi di posta elettronica crittografati elaborati da Mimecast Secure Email Gateway

Sommario

Introduzione

Questo documento descrive un problema con i messaggi di posta elettronica crittografati del servizio Cisco Secure Email Encryption (in precedenza Cisco Registered Envelope Service) se l'entità che riceve i messaggi ha un gateway di posta elettronica sicuro Mimecast e le riscritture degli URL sono abilitate.

Problema

Per quanto riguarda l'integrazione di Mimecast e Cisco Secure Email Encryption, sono stati osservati due comportamenti distinti nel campo.

- Mimecast trasforma la barra rovesciata in una barra in avanti, con conseguente errore di reindirizzamento del browser.
- Mimecast riscrive l'URL nell'allegato e danneggia il payload.

Problema di reindirizzamento del browser

Descrizione

Mimecast Secure Email Gateway cambia la barra rovesciata in una barra in avanti nell'allegato securedoc.html, che danneggia il payload e impedisce agli utenti finali di aprire i messaggi.

Sintomi

I sintomi generali includono utenti finali che non sono in grado di immettere la password o che il campo della password genera errori.

Identificazione del problema

1. Chiedere agli utenti finali interessati di condividere il file **securedoc.html**

2. Aprire il file **securedoc.html** nell'editor di testo desiderato (ad esempio, Notepad++) o condividerlo con Cisco TAC e cercare la stringa: **ReindirizzamentoBrowser**

3. Esaminare l'URL completo con **BrowserRedirect** e verificare se alla fine è presente una barra rovesciata o avanti.

r. URL corretto (termina con una barra rovesciata) - java.sun.com/webapps/getjava/**BrowserRedirect**

b. URL con problemi (termina con una barra) - java.sun.com/webapps/getjava/**BrowserRedirect/**

4. Un URL non corretto termina con una barra e ci consente di confermare il comportamento che causa il problema.

Soluzione

1. È stato rilasciato un aggiornamento del motore di crittografia (PXE) che include una correzione che risolve il problema. Eseguire **updatenow** force dalla CLI per attivare l'aggiornamento.

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

Success - Force update for all components requested
```

2. Una volta avviato un aggiornamento, è possibile utilizzare il comando **encryptionstatus** per verificare che l'aggiornamento sia stato applicato.

```
(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. Se l'operazione ha esito positivo, l'output del modulo di gestione PXE visualizza la data e l'ora correnti.


```
(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 di riscrittura URL

Descrizione

Mimecast Secure Email Gateway riscrive gli URL nell'allegato **securedoc.html**, danneggiando il payload e impedendo agli utenti di aprire i messaggi.

Sintomi

I sintomi generali includono utenti finali che non sono in grado di immettere la password o che il campo della password genera errori.

Identificazione del problema

1. Chiedere agli utenti finali interessati di condividere il file **securedoc.html**

2. Aprire il file **securedoc.html** nell'editor di testo desiderato (ad esempio, Notepad++) o condividerlo con Cisco TAC e cercare la stringa: **protect-us.mimecast.com**

3. Esaminare gli URL riscritti e fare riferimento all'immagine per un confronto prima e dopo il confronto.

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. Quando l'allegato securedoc.html viene inviato tramite Mimecast Secure Email Gateway, gli URL a cui si fa riferimento vengono riscritti in modo errato, causando l'interruzione della sintassi HTML. Per questo motivo, gli utenti finali non sono in grado di aprire le e-mail crittografate.

Ad esempio:

https://res.cisco.com:443/websafe/help?topic=AddrNotShown',**{'localeUI':getLocale()})** viene riscritto in https://protect-us.mimecast.com/s/fQ-lCkRMXRUn3B5DDIQIC_L?domain=res.cisco.com**':getLocale()})**. Come si può vedere, dopo la riscrittura degli URL il campo **localeUI** viene rimosso.

Soluzioni

1. Inoltra l'e-mail in questione a mobile@res.cisco.com. Una volta ricevuti, gli utenti finali potrebbero fare clic sul link e decrittografare correttamente l'e-mail.

o

2. Attivare la funzione Easy Open. I messaggi di posta elettronica crittografati verrebbero inviati ai destinatari con un collegamento di visualizzazione nel corpo del messaggio. Gli utenti finali potranno quindi cliccare sul link e decriptare l'e-mail.

o

3. Ignorare il dominio del mittente di res.cisco.com su Mimecast Secure Email Gateway.

Ulteriori informazioni

Documentazione di Cisco Secure Email Gateway

- Note sulla release
- Guida dell'utente
- Guida di riferimento CLI

- Guide alla programmazione API per Cisco Secure Email Gateway
- Open Source utilizzato in Cisco Secure Email Gateway
- Guida all'installazione di Cisco Content Security Virtual Appliance (include vESA)

Documentazione su Secure Email Cloud Gateway

- Note sulla release
- Guida dell'utente

Documentazione di Cisco Secure Email e Web Manager

- Note sulla versione e matrice di compatibilità
- Guida dell'utente
- Guide alla programmazione API per Cisco Secure Email e Web Manager
- Guida all'installazione di Cisco Content Security Virtual Appliance (include vSMA)

Documentazione del prodotto Cisco Secure

- Architettura di denominazione del portafoglio Cisco Secure