

トラブルシューティング : Mimecast Secure Email Gatewayで処理された暗号化された電子メールを開くことができない

内容

[概要](#)

[問題](#)

[ブラウザリダイレクトの問題](#)

[説明](#)

[症状](#)

[問題の特定](#)

[解決方法](#)

[URL書き換えの問題](#)

[説明](#)

[症状](#)

[問題の特定](#)

[解決方法](#)

[追加情報](#)

[Cisco Secure Email Gatewayのドキュメント](#)

[Secure Email Cloud Gatewayドキュメント](#)

[Cisco Secure Email and Web Managerのドキュメント](#)

[Cisco Secure製品ドキュメント](#)

概要

このドキュメントでは、電子メールを受信するエンティティにMimecastセキュア電子メールゲートウェイがあり、URLの書き換えが有効になっている場合の、Cisco Secure Email Encryption Service(SEEM) (以前のCisco Registered Envelope Service) で暗号化された電子メールの問題について説明します。

問題

MimecastとCisco Secure Email Encryptionの統合に関して、フィールドでは2つの異なる動作が確認されています。

- Mimecastは、バックスラッシュをスラッシュに変更し、ブラウザのリダイレクトに失敗します。
- Mimecastは添付ファイルのURLを書き換え、ペイロードを破損します。

ブラウザリダイレクトの問題

説明

Mimecast Secure Email Gatewayは、`securedoc.html`添付ファイルのバックスラッシュをスラッシュに変更します。これにより、ペイロードが破損し、エンドユーザがメッセージを開けなくなります。

症状

一般的な症状には、パスワードを入力できないエンドユーザや、パスワードフィールドでエラーが発生するエンドユーザなどがあります。

Password



問題の特定

- 1.影響を受けるエンドユーザに、`securedoc.html`の共有を要求します。
- 2.テキストエディタ(たとえば、Notepad++)で`securedoc.html`ファイルを開くか、Cisco TACと共有して文字列を検索します。**BrowserRedirect**
3. **BrowserRedirect**で完全なURLを確認し、末尾にバックスラッシュまたはフォワードスラッシュがあるかどうかを確認します。
 - a.正しいURL (バックスラッシュで終わる)
`:java.sun.com/webapps/getjava/BrowserRedirect\`
 - b.問題のあるURL (スラッシュで終わる)
`:java.sun.com/webapps/getjava/BrowserRedirect/`
- 4.誤ったURLはスラッシュで終わり、問題のある動作を確認することができます。

解決方法

- 1.暗号化(PXE)エンジンのアップデートがリリースされ、この問題を解決する修正が含まれています。CLIから`updatenow force`を実行して、アップデートをトリガーしてください。

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

```
Success - Force update for all components requested
```

- 2.アップデートが開始されたら、`encryptionstatus`コマンドを使用して、アップデートが適用されたことを確認できます。

```
(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.成功すると、PXEエンジンの出力に現在の日付と時刻が表示されます。

```
(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
```

URL書き換えの問題

説明

Mimecast Secure Email Gatewayは、**securedoc.html**添付ファイルのURLを書き換えます。これにより、ペイロードが破損し、エンドユーザがメッセージを開けなくなります。

症状

一般的な症状には、パスワードを入力できないエンドユーザや、パスワードフィールドでエラーが発生するエンドユーザなどがあります。

Password



Error



Error

問題の特定

- 1.影響を受けるエンドユーザに、**securedoc.html**の共有を要求します。
- 2.テキストエディタ(たとえば、Notepad++)で**securedoc.html**ファイルを開くか、Cisco TACと共有して文字列を検索します。**protect-us.mimecast.com**
- 3.書き換えられたURLを確認し、前後の比較については画像を参照してください。

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-ICkRMXRUn3B5DDIQIC_L?domain=res.cisco.com%27:getLocale()%7d
https://res.cisco.com:443/websafe/help?topic=AddrNotShown'	https://protect-us.mimecast.com/s/K-wsCIY6EYioqEXWwtq8lgM?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-wsCIY6EYioqEXWwtq8lgM?domain=res.cisco.com'
https://res.cisco.com:443/keyserver/keyserver	https://protect-us.mimecast.com/s/8FnrCpYVLyZeoAggFkH5wE?domain=res.cisco.com

4. securedoc.html添付ファイルがMimecastセキュア電子メールゲートウェイを介して送信されると、参照URLが誤って書き換えられ、HTML構文が中断されます。このため、エンドユーザは暗号化された電子メールを開くことができません。

以下に、いくつかの例を示します。

https://res.cisco.com:443/websafe/help?topic=AddrNotShown',('localeUI':getLocale()))は
https://protect-us.mimecast.com/s/fQ-
ICkRMXRUn3B5DDIQIC_L?domain=res.cisco.com':getLocale()))に書き換えられます。URLが書き換えられると、localeUIフィールドは削除されていることがわかります。

解決方法

1. 問題の電子メールをmobile@res.cisco.comに転送します。受信すると、エンドユーザはリンクをクリックしてEメールを正常に復号化できます。

または

2. Easy Open機能を有効にします。暗号化された電子メールは、電子メールの本文に表示リンクが含まれた受信者に送信されます。これにより、エンドユーザはリンクをクリックして電子メールを復号化できるようになります。

または

3. Mimecast Secure Email Gatewayでres.cisco.comの送信者ドメインをバイパスします。

追加情報

Cisco Secure Email Gatewayのドキュメント

- [リリースノート](#)
- [ユーザガイド](#)
- [CLIリファレンスガイド](#)
- [Cisco Secure Email GatewayのAPIプログラミングガイド](#)
- [Cisco Secure Email Gatewayで使用されるオープンソース](#)

- [Ciscoコンテンツセキュリティ仮想アプライアンスインストールガイド \(vESAを含む\)](#)

Secure Email Cloud Gatewayドキュメント

- [リリースノート](#)
- [ユーザガイド](#)

Cisco Secure Email and Web Managerのドキュメント

- [リリースノートと互換性マトリクス](#)
- [ユーザガイド](#)
- [Cisco Secure Email and Web ManagerのAPIプログラミングガイド](#)
- [Ciscoコンテンツセキュリティ仮想アプライアンスインストールガイド \(vSMAを含む\)](#)

Cisco Secure製品ドキュメント

- [Cisco Secureポートフォリオの命名アーキテクチャ](#)