Fehler beim Öffnen verschlüsselter E-Mails, die von Mimecast Secure Email Gateway verarbeitet wurden

Inhalt

Einleitung

In diesem Dokument wird ein Problem mit verschlüsselten E-Mails des Cisco Secure Email Encryption Service (ehemals Cisco Registered Envelope Service) beschrieben, wenn die Einheit, die die E-Mails empfängt, über ein Mimecast Secure Email Gateway verfügt und URL-Umschreibungen aktiviert sind.

Problem

Bei der Integration von Mimecast und Cisco Secure Email Encryption wurden vor Ort zwei unterschiedliche Verhaltensweisen beobachtet.

- Mimecast ändert den umgekehrten Schrägstrich in einen umgekehrten Schrägstrich, was zu einem Fehler bei der Browserumleitung führt.
- Mimecast schreibt die URL in der Anlage neu und beschädigt die Payload.

Problem mit Browser-Umleitung

Beschreibung

Mimecast Secure Email Gateway ändert den umgekehrten Schrägstrich in einen Schrägstrich im Anhang "securedoc.html", wodurch die Payload beschädigt wird und die Endbenutzer keine Nachrichten öffnen können.

Symptome

Zu den allgemeinen Symptomen gehören Endbenutzer, die ihr Kennwort nicht eingeben können oder die im Kennwortfeld Fehler eingeben.

Identifizieren des Problems

1. Fordern Sie alle betroffenen Endbenutzer an, die Datei **securedoc.html** freizugeben.

2. Öffnen Sie die Datei **securedoc.html** in Ihrem gewünschten Texteditor (z. B. Notepad++), oder geben Sie sie an das Cisco TAC weiter, und suchen Sie nach der Zeichenfolge: **BrowserUmleiten**

3. Überprüfen Sie mit dem **BrowserRedirect** die vollständige URL, und stellen Sie sicher, dass am Ende ein Schrägstrich oder ein Schrägstrich steht.

antwort: Richtige URL (endet mit umgekehrtem Schrägstrich) - java.sun.com/webapps/getjava/**BrowserRedirect**

b. Problematische URL (endet mit einem Schrägstrich) - java.sun.com/webapps/getjava/**BrowserRedirect/**

4. Eine falsche URL endet mit einem Schrägstrich und ermöglicht uns, das problematische Verhalten zu bestätigen.

Lösung

1. Ein Update des Verschlüsselungsmoduls (PXE) wurde veröffentlicht, das einen Fix enthält, der das Problem löst. Führen Sie **updatenow** force über die CLI aus, um das Update auszulösen.

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

Success - Force update for all components requested
```

2. Nachdem ein Update gestartet wurde, können Sie mit dem Befehl **encryptionstatus** bestätigen, dass das Update angewendet wurde.

```
(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. Bei Erfolg zeigt die Ausgabe der PXE Engine das aktuelle Datum und die aktuelle Uhrzeit an.

```
(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
```

Problem mit URL-Umschreibung

Beschreibung

Mimecast Secure Email Gateway schreibt die URLs in der Anlage **securedoc.html** um, wodurch die Payload beschädigt wird und die Endbenutzer keine Nachrichten öffnen können.

Symptome

Zu den allgemeinen Symptomen gehören Endbenutzer, die ihr Kennwort nicht eingeben können oder die im Kennwortfeld Fehler eingeben.

Identifizieren des Problems

1. Fordern Sie alle betroffenen Endbenutzer an, die Datei **securedoc.html** freizugeben.

2. Öffnen Sie die Datei **securedoc.html** in Ihrem gewünschten Texteditor (z. B. Notepad++), oder geben Sie sie an das Cisco TAC weiter, und suchen Sie nach der Zeichenfolge: **protect-us.mimecast.com**

3. Überprüfen Sie die neu geschriebenen URLs, und verweisen Sie für einen Vorher-Nachher-Vergleich auf das Bild.

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. Wenn der Anhang "securedoc.html" über das Mimecast Secure Email Gateway gesendet wird, werden die URLs, auf die verwiesen wird, falsch geschrieben, wodurch die HTML-Syntax unterbrochen wird. Daher können die Endbenutzer die verschlüsselten E-Mails nicht öffnen.

Beispiele:

https://res.cisco.com:443/websafe/help?topic=AddrNotShown',**{'localeUI':getLocale()})** wird in https://protect-us.mimecast.com/s/fQ-lCkRMXRUn3B5DDIQIC_L?domain=res.cisco.com':**getLocale()} umgeschrieben.** Wie Sie sehen, wird das **localeUI-**Feld nach dem Umschreiben der URLs entfernt.

Lösungen

1. Leiten Sie die betreffende E-Mail an mobile@res.cisco.com weiter. Nach Erhalt können die Endbenutzer auf den Link klicken und die E-Mail erfolgreich entschlüsseln.

Oder

2. Aktivieren Sie die Easy Open-Funktion. Verschlüsselte E-Mails werden an die Empfänger gesendet, die über einen View-Link im Text der E-Mail verfügen. Die Endbenutzer können dann auf den Link klicken und die E-Mail entschlüsseln.

Oder

3. Umgehen Sie die Absenderdomäne von res.cisco.com auf dem Mimecast Secure Email Gateway.

Zusätzliche Informationen

Cisco Secure Email Gateway-Dokumentation

- Versionshinweise
- Benutzerhandbuch

- CLI-Referenzhandbuch
- API-Programmierhandbücher für Cisco Secure Email Gateway
- Open Source für Cisco Secure Email Gateway
- Installationsanleitung für die Cisco Content Security Virtual Appliance (mit vESA)

Secure Email Cloud Gateway - Dokumentation

- Versionshinweise
- Benutzerhandbuch

Cisco Secure Email und Web Manager-Dokumentation

- Versionshinweise und Kompatibilitätsmatrix
- Benutzerhandbuch
- API-Programmierhandbücher für Cisco Secure Email und Web Manager
- Cisco Content Security Virtual Appliance Installationshandbuch (einschl. vSMA)

Cisco Secure-Produktdokumentation

- Cisco Secure Portfolio Naming Architecture