Cisco Secure Email Gateway SMTPの密輸に関する脆弱性レポートへの応答

内容

はじめに

このドキュメントでは、2023年12月18日にSEC Consultが発行した「SMTPの密輸 – 世界中の電子メールのスプーフィング」で説明されている攻撃に対して、Cisco Secure Emailがどのように対処するかについて詳しく説明します。

SEC Consult Vulnerability Labと共同で行った研究プロジェクトの中で、Timo Longin(@timolongin)は、さらに別のインターネットプロトコルであるSimple Mail Transfer Protocol(SMTP)の新しいエクスプロイトテクニックを発見しました。脅威アクターは、世界中の脆弱なSMTPサーバを悪用して任意の電子メールアドレスから悪意のある電子メールを送信し、ターゲットを絞ったフィッシング攻撃を可能にする可能性があります。この脆弱性は、不正利用の性質上、SMTPの密輸と呼ばれていました。

シスコでは、このホワイトペーパーに記載されている攻撃が、設定されたセキュリティフィルタのバイパスに使用される可能性があることを示す証拠を一切発見していません。

技術背景

SMTPプロトコルとメッセージ形式の詳細を取り上げることなく、コンテキストを取得するためにRFC 5322の一部のセクションを参照することが重要です。

セクション2.1では、CRLF文字シーケンスを、メッセージの異なるセクション間で使用されるセパレータとして定義しています。

メッセージは文字の行に分割されます。行は、キャリッジリターンと改行の2文字で区切られた一連の文字です。つまり、キャリッジリターン(CR)文字（ASCII値13）の直後に改行(LF)文字（ASCII値10）が続きます。（通常、キャリッジリターン/ラインフィードのペアは、このドキュメントでは「CRLF」と記述します）。

セクション2.3では、メッセージ本文の形式について詳しく説明します。また、CRおよびLF文字を本体の一部として独立して送信してはならないことを明確に規定しています。このような設定を行っているサーバは、RFCに準拠していません。

メッセージの本文は、US-ASCII文字の行です。身体に関する唯一の2つの制限は以下の通りである：

- CRとLFは、CRLFとして同時に出現する必要があります。CRとLFが独立して本文に出現してはなりません。
- 本文の行は、998文字に制限する必要があります。また、CRLFを除き、78文字に制限する必要があります。

ただし、同じドキュメントのセクション4.1では、それほど限定的ではない旧リビジョンのRFCからの廃止された構文に言及して、フィールドでの多くの実装が正しい構文を使用していないことを認めています。

Bare CRとBare LFは、2つの異なる意味でメッセージに表示されます。多くの場合、行区切りを示すためにCRLFの代わりにベアCRまたはベアLFが不適切に使用されます。また、単にUS-ASCIIの制御文字としてCRやLFを使用し、従来のASCIIの意味を使用する場合もあります。

要約すると、RFC 5322によれば、適切な形式のSMTPメッセージは次の例のようになります。

```
ehlo sender.example\r\n
mail FROM:<user@sender.example>\r\n
rcpt TO:<user@receiver.example>\r\n
data\r\n
From: <user@sender.example>\r\n
To: <user@receiver.example>\r\n
Subject: Example\r\n
\r\n
lorem ipsum\r\n
\r\n. \r\n
```

このドキュメントでは、RFCのセクション4.1で説明されている例外を利用して、送信側サーバと受信側サーバのセキュリティ対策をバイパスするために、新しいメッセージを本文の一部に挿入したり、メッセージをこっそり処理したりすることを試みています。この目的は、不正メッセージがセキュリティチェックをバイパスすることです。これは、これらのチェックがメッセージの途中で実行され、その後で回線が空き状態になるためです。例：

<#root>

```
ehlo sender.example\r\n
mail FROM:<user@sender.example>\r\n
rcpt TO:<user@receiver.example>\r\n
data\r\n
From: <user@sender.example>\r\n
To: <user@receiver.example>\r\n
Subject: Example\r\n
\r\n
```

```
lorem ipsum\r\n
\n. \r\n
mail FROM:<malicious@malicious.example>
\r\n
rcpt TO:<user@receiver.example>
\r\n
data
\r\n
From: <malicious@malicious.example>
\r\n
To: <user@receiver.example>
\r\n
Subject: Malicious
\r\n
\r\n
Malicious content
\r\n
\r\n
.
\r\n
```

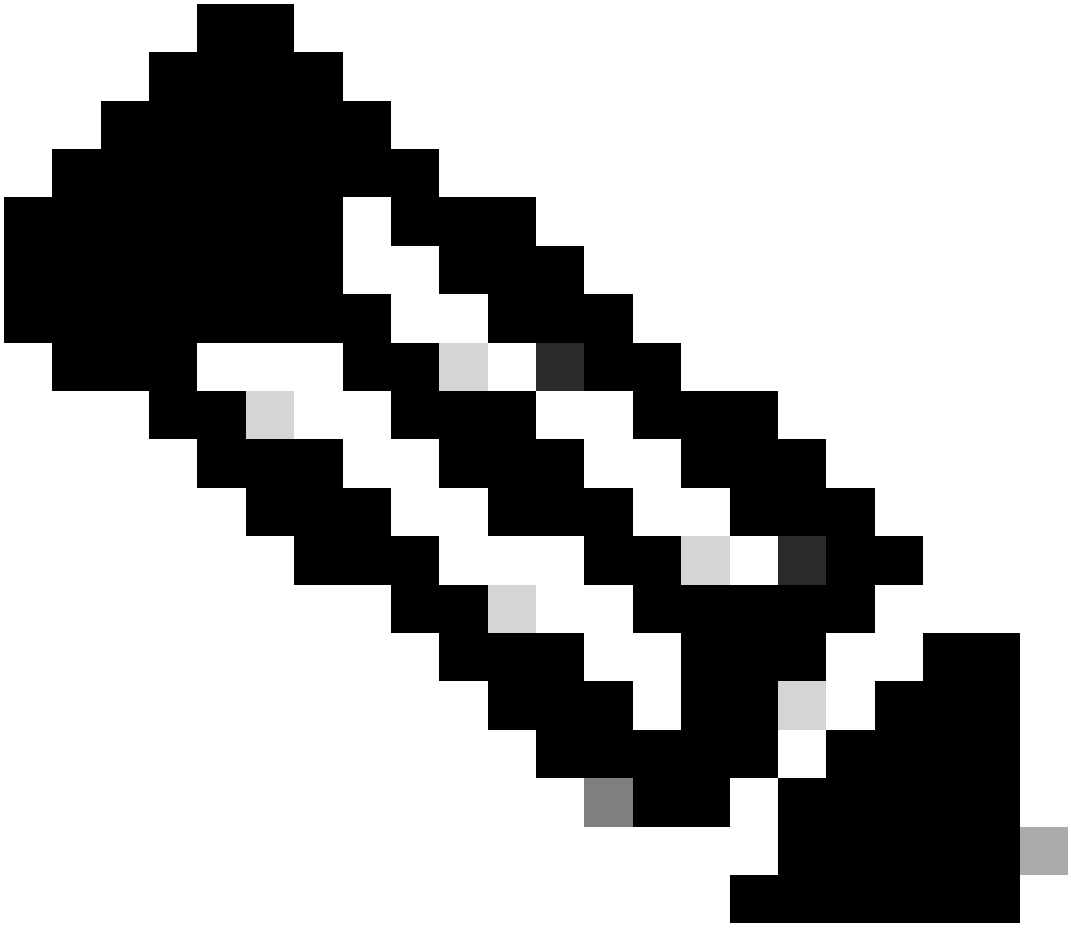
Cisco Secure Mailの動作

Cisco Secure MailでSMTPリスナーを設定する際には、CRおよびLF文字の処理方法を決定する3つの設定オプションがあります。

ベアCRおよびLF文字のクリーンメッセージ（デフォルト）

デフォルトオプションを選択すると、Cisco Secure Mailは着信メッセージ内のすべてのCRおよびLF文字を正しいCRLFシーケンスに置き換えます。

例に示すような密輸コンテンツを含むメッセージは2つの個別のメッセージとして扱われ、すべてのセキュリティチェック(Sender Policy Framework(SPF)、Domain-based Message Authentication, Reporting & Conformance(DMARC)、AntiSpam、Antivirus、Advanced Malware Protection(AMP)、コンテンツフィルタなど)がそれぞれで独立して実行されます。



注：この設定では、攻撃者が別のユーザになりすましてメッセージを密輸できる可能性があることに注意してください。攻撃者は、複数のドメインをホストする発信元サーバが、サーバでホストされているその他のドメインの1つからユーザになりすまして密輸された電子メールのSPFチェックを通過させる可能性があるため、この状況に大きな影響を与える可能性があります。

CR文字またはLF文字を含むメッセージの拒否

この設定オプションは、RFCへの厳密な準拠を強制します。CR文字またはLF文字を含むメッセージは拒否されます

この設定により密輸のシナリオは防止されますが、RFCに準拠していないサーバからの正当な電子メールもドロップされます。

CR文字またはLF文字を含むメッセージを許可する（非推奨）

最終的な設定では、Cisco Secure MailはASCIIの意味を使用してCRおよびLFの文字を処理します

。メッセージ本文は、密輸されたコンテンツを含め、現状のまま配信されます。

このメッセージは本体の一部として扱われるため、このメッセージの一部に含まれる添付ファイルがCisco Secure Mailで検出されない場合があります。これにより、ダウンストリームデバイスでセキュリティ上の問題が発生する可能性があります。このオプションは使用されなくなりました。

推奨設定

シスコでは、デフォルトの「Clean messages of bare CR and LF characters」オプションを使用することを推奨しています。このオプションを使用すると、セキュリティと相互運用性の間で最適な妥協が可能になるためです。ただし、この設定を使用するお客様は、密輸されたコンテンツに関するセキュリティの影響を認識する必要があります。RFCへの準拠を求めるお客様は、相互運用性の問題があることを認識したうえで、「CRまたはLF文字のみのメッセージを拒否する」ことを選択する必要があります。

いずれの場合でも、着信メッセージの送信者を検証するために、SPF、DomainKeys Identified Mail(DKIM)、DMARCなどの機能を設定し、使用することを強く推奨します。

AsyncOSリリース15.0.2および15.5.2以降には、メッセージ終了RFC標準に準拠していないメッセージの識別とフィルタリングに役立つ新機能が追加されています。無効なメッセージ終了シーケンス(EOF)を含むメッセージを受信すると、Eメールゲートウェイは、メッセージ終了RFC標準に準拠するメッセージを受信するまで、その接続内のすべてのメッセージID(MID)にX-Ironport-Invalid-End-Of-Message Extension Header(X-Header)を追加します。お客様は、コンテンツフィルタを使用して「X-Ironport-Invalid-End-Of-Message」ヘッダーを探し、これらのメッセージに対して実行するアクションを定義できます。

よく寄せられる質問（FAQ）

Cisco Secure Mailは、上記の攻撃に対して脆弱ですか。
技術的には、そうです。メールにCR文字やLF文字が含まれている場合、メールの一部を2通目のメールとして扱わせることが可能です。ただし、2番目の電子メールは個別に分析されるため、2つの異なるメッセージを送信することと同じ動作になります。シスコでは、このホワイトペーパーに記載されている攻撃が、設定されたセキュリティフィルタのバイパスに使用される可能性があることを示す証拠を一切発見していません。

バイパスされたSPFおよびDKIMチェックの例を示します。フィルタがバイパスされていないとシスコが主張するのはなぜですか。
これらの例では、SPFチェックは期待どおりに実行されますが、送信側サーバが複数のドメインを所有しているため、チェックに合格します。

推奨される設定は何ですか。
お客様に最も適した選択肢は、お客様固有の要件に依存します。推奨されるオプションは、デフォルトの「クリーン」構成または「拒否」代替です。

「Reject」オプションを選択すると、誤検出が発生しますか。
「拒否」機能は、電子メールがRFC標準に準拠しているかどうかの評価を開始します。電子メー

ルがRFC標準に準拠していない場合は、拒否されます。正規の電子メールであっても、電子メールがRFC標準に準拠していない場合は拒否できます。

この問題を力バーしているソフトウェアの不具合はありますか。
Cisco Bug ID CSCwh10142に記載されています。

このトピックに関する詳細情報の入手方法を教えてください。
フォローアップの質問は、Technical Assistance Center(TAC)のケースを通じて行うことができます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。