對思科安全郵件網關SMTP走私漏洞報告的響應

目錄

簡介

背景資訊

技術背景

Cisco Secure Mail行為

- 清除空的CR和LF字元的消息（預設）
- 拒絕包含空白CR或LF字元的訊息
- 允許包含純CR或LF字元的訊息（已停用）

建議的配置

常見問題

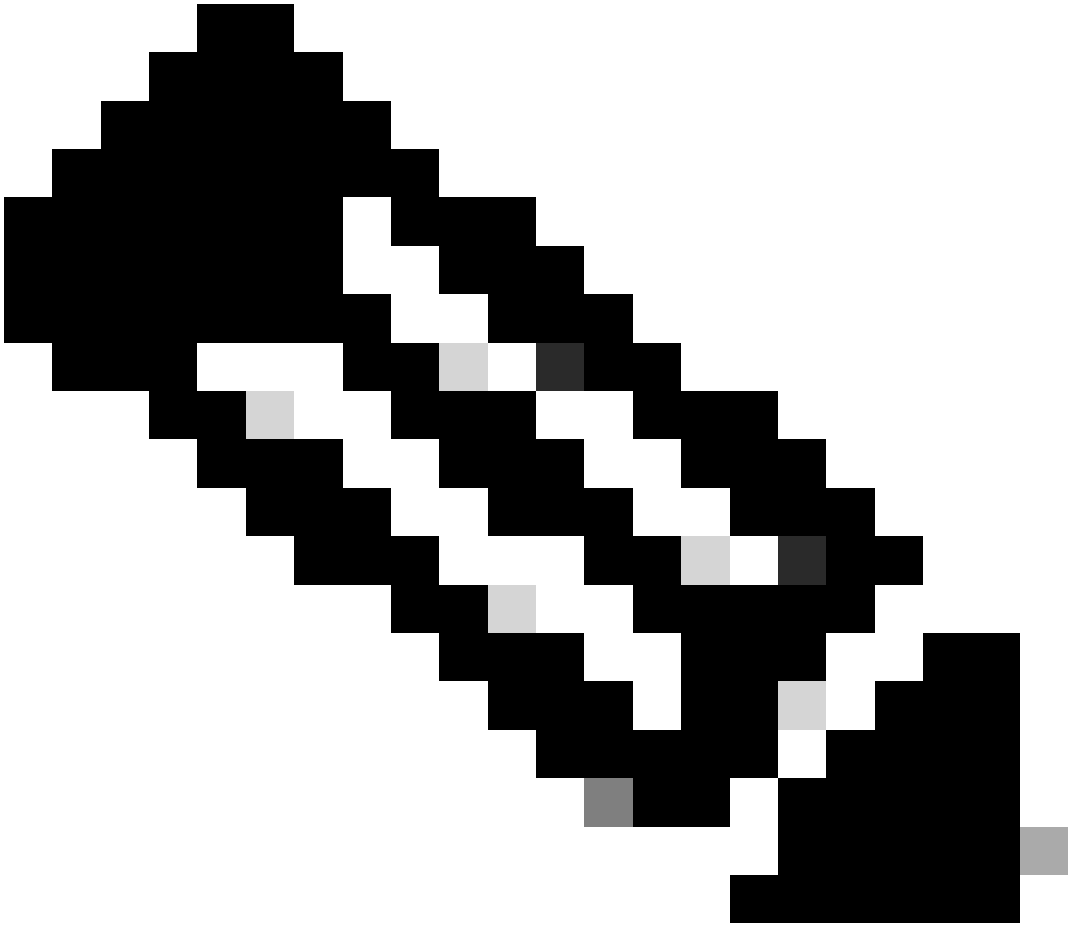
- Cisco Secure Mail是否容易遭受所述攻擊？
- 該文檔提供了繞過SPF和DKIM檢查的示例。為什麼思科說沒有繞過過濾器？
- 建議的配置是什麼？
- 選擇「拒絕」選項是否會導致誤報？
- 是否存在涵蓋此問題的軟體Bug？
- 如何獲得有關此主題的更多資訊？

簡介

本文檔提供了有關Cisco安全電子郵件如何針對SMTP走私-欺騙全球電子郵件（由SEC Consult於2023年12月18日發佈）中描述的攻擊型別執行操作的詳細資訊。

背景資訊

在與SEC Consult Vulnerability Lab合作進行的一項研究專案中，Timo Longin (@timolongin)發現了另一種新的網際網路協定利用技術— SMTP(簡單郵件傳輸協定)。威脅實施者可能會利用全球範圍內易受攻擊的SMTP伺服器從任意電子郵件地址傳送惡意電子郵件，從而允許有針對性的網路釣魚攻擊。由於漏洞本身的性質，此類漏洞稱為SMTP走私。



注意：思科尚未發現任何證據表明白皮書中所描述攻擊可用於繞過任何已配置的安全過濾器。

技術背景

在不詳細介紹SMTP協定和消息格式的情況下，檢視RFC 5322 的幾部分以得到一些上下文是很重要的。

第2.1節將CRLF字元序列定義為消息不同部分之間使用的分隔符。

訊息會分成字元行。行是一系列字元，用回車符和換行符分隔；即回車符(CR)字元（ASCII值13）後緊跟換行符(LF)字元（ASCII值10）。（在此檔案中，換行符/換行符配對通常寫為「CRLF」。）

第2.3節更詳細地說明了消息主體的格式。它明確宣告CR和LF字元絕不能作為身體的一部分單獨傳送。執行此操作的任何伺服器都不符合RFC。

消息正文只是一行US-ASCII字元。對主體的唯一兩個限制如下：

- CR和LF只能以CRLF的形式同時出現；它們不能單獨出現在主體中。
- 正文中的字元行數必須限制為998個字元，且應限制為78個字元（CRLF除外）。

然而，同一文檔的第4.1節介紹了先前版本的RFC中不再受限制的語法，該節承認欄位中的許多實現沒有使用正確的語法。

空的CR和空的LF出現在具有兩種不同含義的消息中。在許多情況下，不正確地使用裸的CR或裸的LF來代替CRLF來指示分隔線。在其它情況下，裸的CR和裸的LF僅用作US-ASCII控制字元，具有傳統的ASCII含義。

根據RFC 5322，總結一下，格式正確的SMTP郵件將如下所示：

```
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
```

本文試圖利用RFC 第4.1節中提到的異常，將新郵件作為正文的一部分插入或「走私」，以繞過傳送或接收伺服器上的安全措施。目標是讓走私郵件繞過安全檢查，因為這些檢查將僅在郵件裸線饋送之前對郵件部分執行。舉例來說：

<#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
```

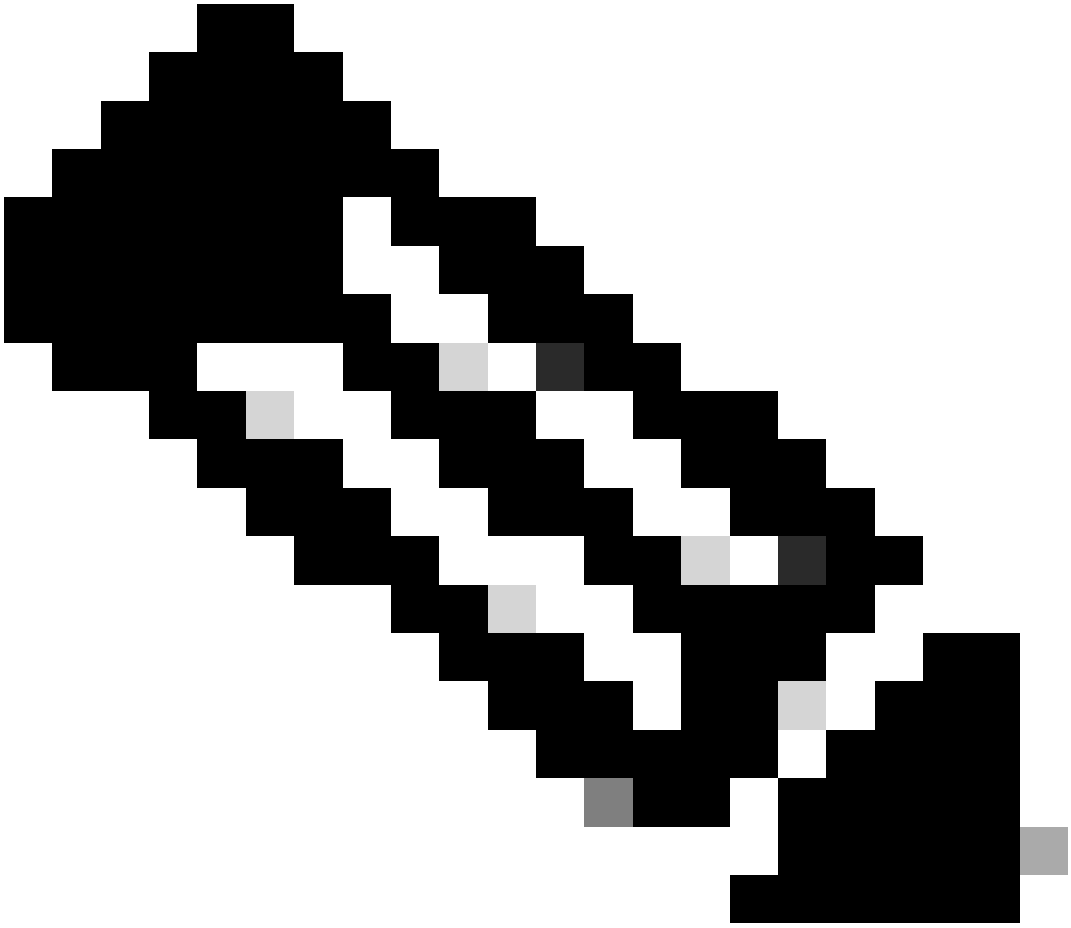
Cisco Secure Mail行為

在Cisco Secure Mail上配置SMTP偵聽程式時，三個配置選項決定了應如何處理空的CR和LF字元。

清除空的CR和LF字元的消息（預設）

選中預設選項後，Cisco Secure Mail會使用正確的CRLF序列替換傳入郵件中的所有空CR和LF字元。

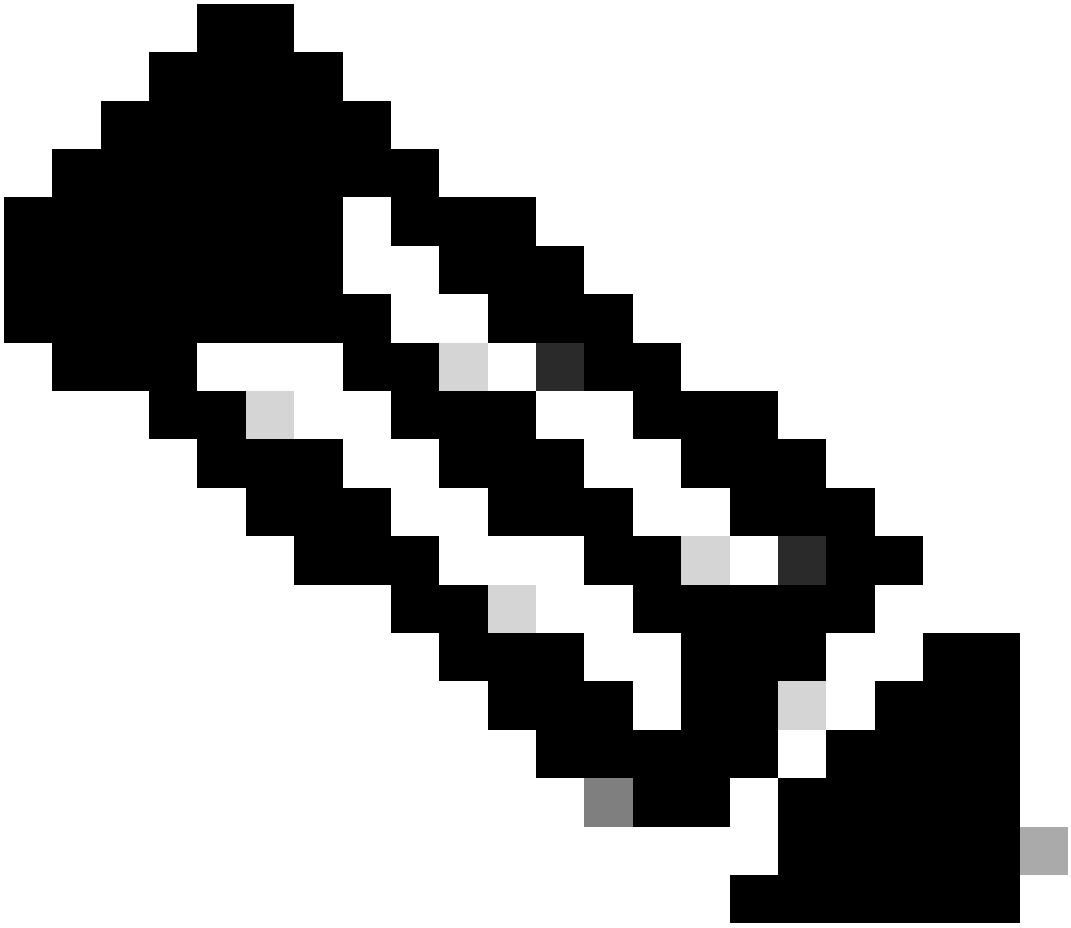
包含走私內容的郵件（如示例中的郵件）將被視為兩個單獨的郵件，並且所有安全檢查(如發件人策略架構(SPF)、基於域的郵件身份驗證、報告和一致性(DMARC)、AntiSpam、防病毒、高級惡意軟體防護(AMP)和內容過濾器)均獨立運行。



注意：客戶應瞭解，使用此配置，攻擊者可能能夠仿冒其他使用者走私郵件。在源伺服器託管多個域的情況下，攻擊者可能會產生更大的影響，因為攻擊者可以模擬來自伺服器上託管的其他域之一的使用者，並且走私郵件上的SPF檢查仍會通過。

拒絕包含空白CR或LF字元的訊息

此配置選項嚴格執行與RFC的合規性。包含空的CR或LF字元的所有消息均會被拒絕。

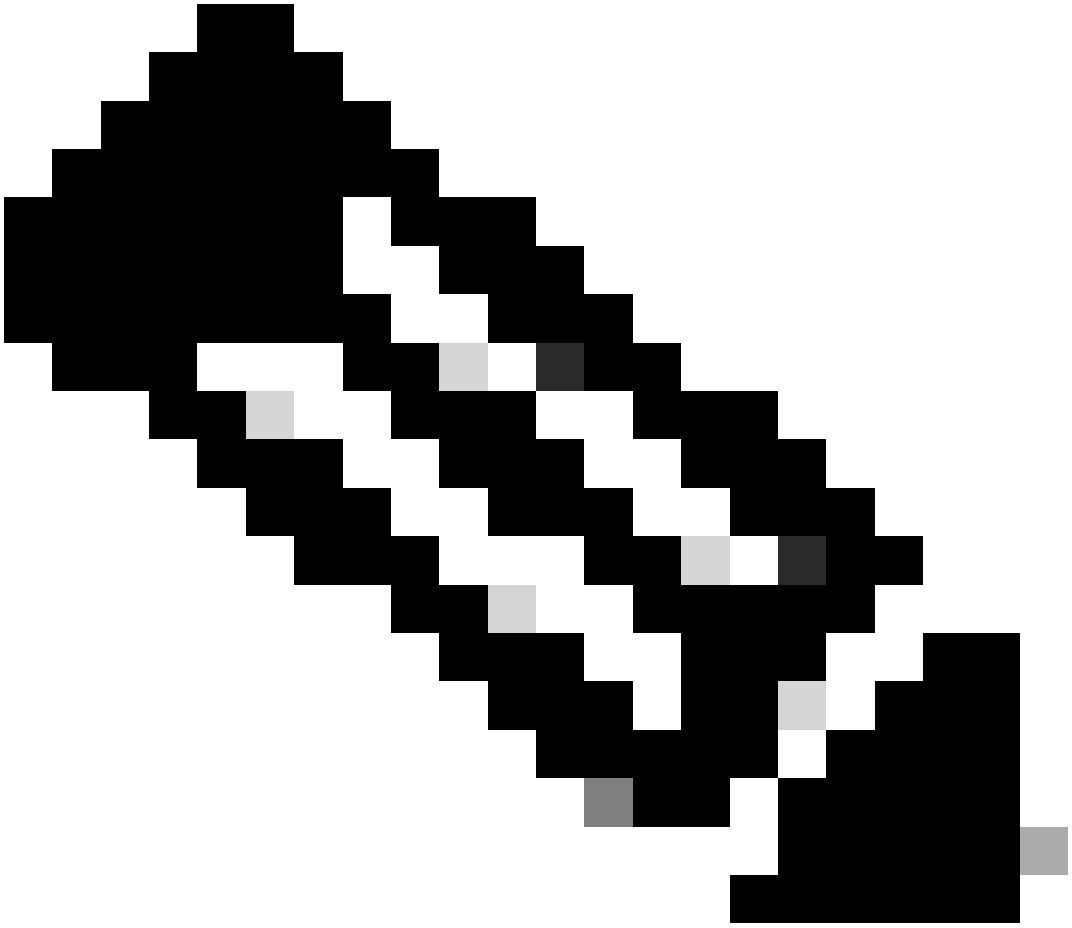


注意：雖然此配置可阻止走私情況，但也會導致來自不符合RFC的伺服器的合法電子郵件被丟棄。

允許包含純CR或LF字元的訊息（已停用）

最終配置使Cisco Secure Mail使用其ASCII意義處理空的CR和LF字元。報文正文按原樣傳送，包括走私內容。

由於該走私郵件被視為內文的一部分，因此Cisco Secure Mail可能無法檢測到作為走私郵件一部分的附件。這可能會在下游裝置上造成安全問題。



注意：此選項已被取代，不再使用。

建議的配置

思科建議使用預設的「清除空閒CR和LF字元的消息」選項，因為它在安全性和互操作性之間提供了最佳折衷方案。但是，使用此設定的客戶應瞭解與走私內容相關的安全影響。希望實施RFC合規性的客戶應選擇「拒絕具有空CR或LF字元的郵件」，同時瞭解潛在的互操作性問題。

在任何情況下，思科強烈建議配置並使用SPF、DomainKeys Identified Mail (DKIM)或DMARC等功能來驗證傳入消息的發件人。

AsyncOS版本15.0.2和15.5.1及更高版本增加了有助於辨識和過濾不符合郵件結尾RFC標準的郵件的新功能。如果接收到具有無效消息結尾序列的消息，電子郵件網關會將X-Ironport-Invalid-End-Of-Message擴展報頭(X-Header)增加到該連線內的所有消息ID (MID)，直到收到符合消息結尾RFC標準的消息為止。客戶可以使用內容過濾器查詢「X-Ironport-Invalid-End-Of-Message」報頭，並定義要對這些郵件執行的操作。

常見問題

Cisco Secure Mail是否容易遭受所述攻擊？

技術上來說，是的。如果郵件中包含空的CR和LF字元，則可能導致將部分電子郵件視為第二封電子郵件。但是，由於第二封電子郵件是獨立分析的，因此其行為相當於傳送兩條單獨的郵件。思科未發現任何證據表明本文中描述的攻擊可用於繞過任何已配置的安全過濾器。

該文檔提供了繞過SPF和DKIM檢查的示例。為什麼思科說沒有繞過過濾器？

在這些示例中，SPF檢查按預期運行，但由於傳送伺服器擁有多個域，導致檢查通過。

建議的配置是什麼？

客戶最適當的選擇取決於其特定需求。建議的選項為預設的「清除」配置或「拒絕」選項。

選擇「拒絕」選項是否會導致誤報？

「拒絕」功能可啟動電子郵件是否符合RFC標準的評估。如果郵件不符合RFC標準，則會被拒絕。如果電子郵件不符合RFC標準，甚至合法電子郵件也可能被拒絕。

是否存在涵蓋此問題的軟體Bug？

報告思科漏洞ID CSCwh10142。

如何獲得有關此主題的更多資訊？

任何後續問題都可以透過技術支援中心(TAC)案例提出。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。