对思科安全邮件网关SMTP走私漏洞报告的响应

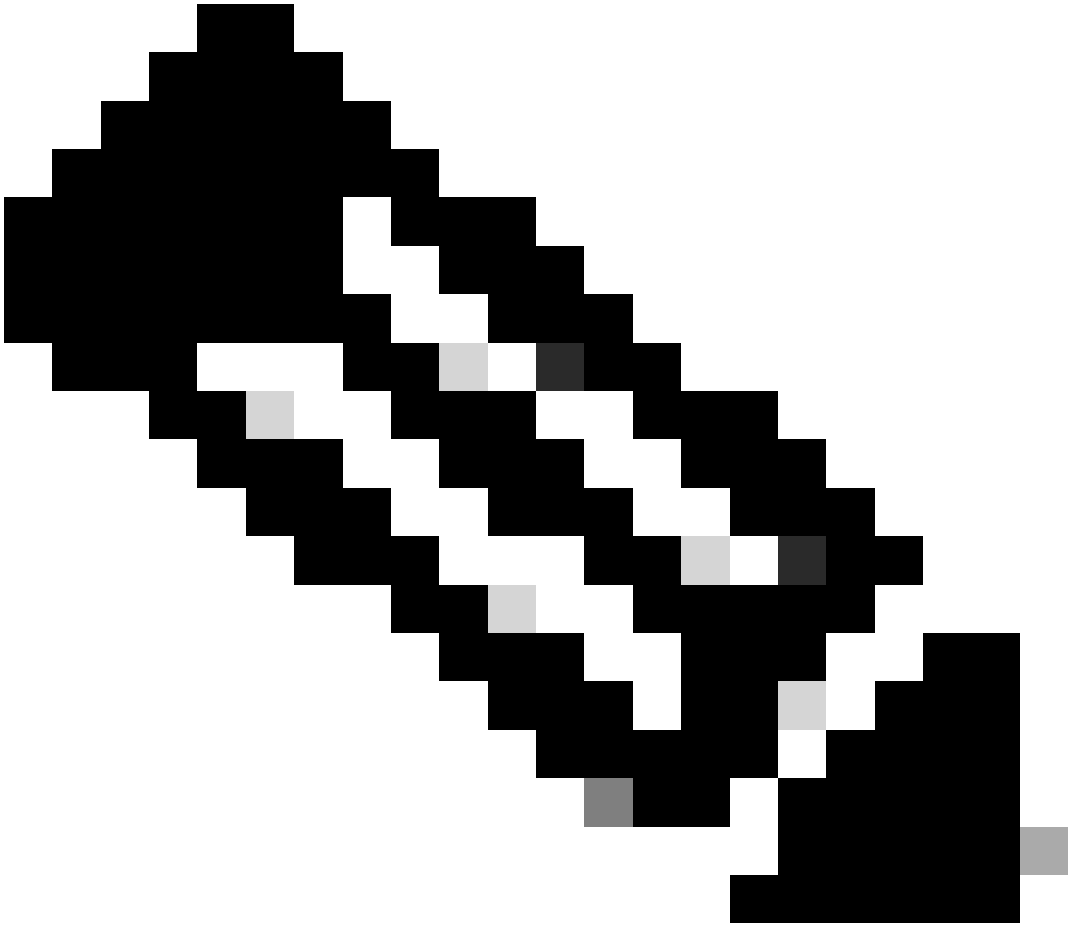
目录

简介

本文档提供了有关Cisco安全电子邮件如何针对SEC Consult于2023年12月18日发布的"SMTP Trusting - Spoofing E-Making Email Worldwide"中所描述攻击类型的详细信息。

背景信息

在与SEC Consult漏洞实验室合作开展的一个研究项目中，Timo Longin (@timolongin)发现了另一种利用互联网协议SMTP(简单邮件传输协议)的新技术。威胁发起者可能会滥用世界各地易受攻击的SMTP服务器，从任意电子邮件地址发送恶意电子邮件，从而实现有针对性的网络钓鱼攻击。由于漏洞本身的性质，此类漏洞被称为SMTP走私。



注意：思科尚未发现任何证据证明本文所述的攻击可用于绕过任何已配置的安全过滤器。

技术背景

不要详细介绍SMTP协议和消息格式，查看RFC 5322 的几部分以获得一些上下文是很重要的。

第2.1节将CRLF字符序列定义为消息不同部分之间使用的分隔符。

消息划分为多行字符。行是一系列字符，由回车符和换行符分隔；即，回车符(CR)字符（ASCII值13）后紧跟换行符(LF)字符（ASCII值10）。（在本文档中，回车/换行符对通常写为“CRLF”。）

第2.3节详细说明了消息正文的格式。它明确声明CR和LF字符绝不应作为身体的一部分单独发送。执行此操作的任何服务器都不符合RFC。

消息正文简称为US-ASCII字符行。对主体的唯一两个限制如下：

- CR和LF必须仅作为CRLF同时出现；它们不能在正文中单独出现。

- 正文中的字符行必须限制为998个字符，并且应限制为78个字符（CRLF除外）。

然而，同一文档的第4.1部分介绍了早期RFC修订版中不再受限制的过时语法，该部分发现该字段中的许多实现没有使用正确的语法。

裸CR和裸LF出现在具有两种不同含义的消息中。在许多情况下，未正确使用纯CR或纯LF来表示线路分隔符，而不是CRLF。在其它情况下，裸CR和裸LF仅用作US-ASCII控制字符，具有传统的ASCII含义。

总之，根据RFC 5322，格式正确的SMTP消息如下所示：

```
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
```

本白皮书尝试利用RFC 4.1节中提及的例外情况，在正文中插入或“走私”新邮件，以绕过发送或接收服务器上的安全措施。目标是让走私邮件绕过安全检查，因为这些检查将仅在裸线馈送之前对邮件的一部分运行。例如：

<#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
```

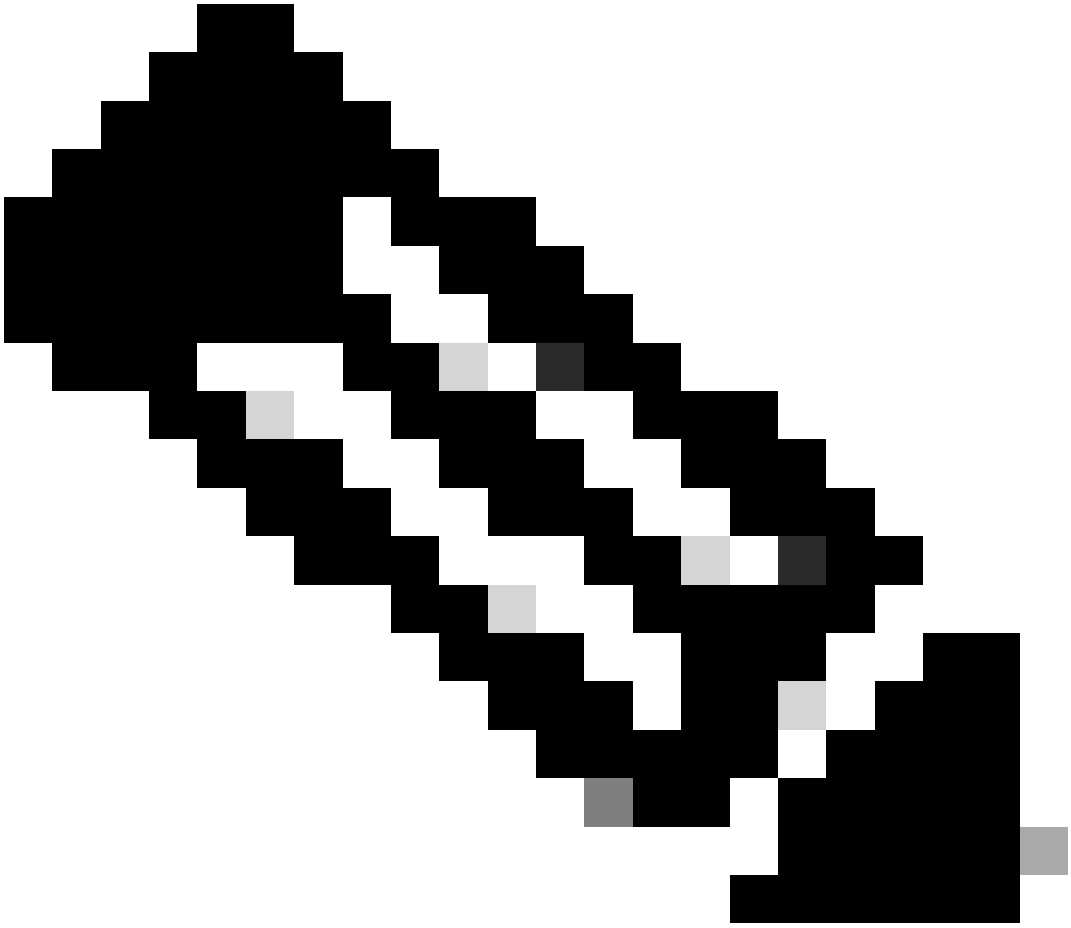
思科安全邮件行为

在Cisco Secure Mail上配置SMTP侦听程序时，三个配置选项确定应如何处理裸CR和LF字符。

正常邮件的CR和LF字符裸露（默认）

选中默认选项后，Cisco Secure Mail将使用正确的CRLF序列替换传入邮件中的所有裸CR和LF字符。

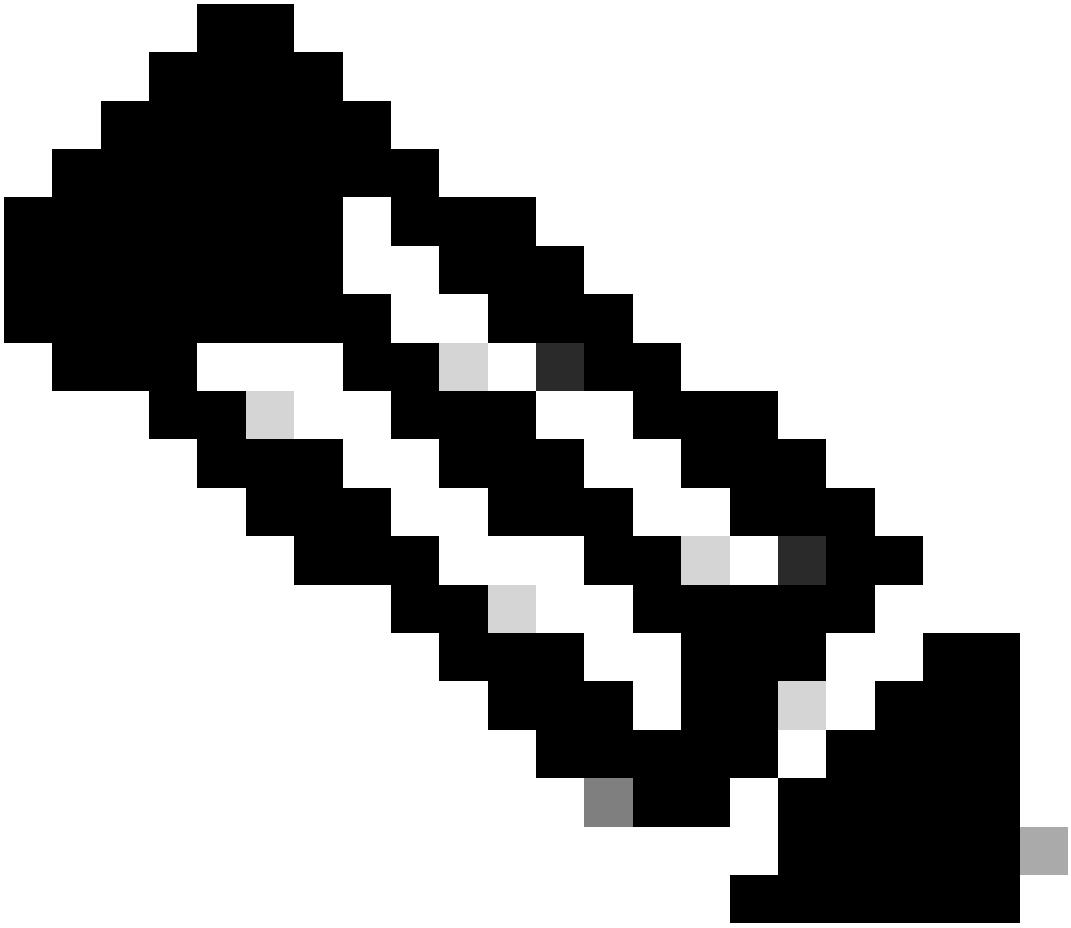
包含走私内容的邮件（如示例中的邮件）将被视为两个单独的邮件，并且所有安全检查(如发件人策略框架(SPF)、基于域的邮件身份验证、报告和一致性(DMARC)、反垃圾邮件、防病毒、高级恶意软件防护(AMP)和内容过滤器)均独立运行。



注意：客户应注意，使用此配置，攻击者可能能够伪装成其他用户而窃取消息。在源服务器托管多个域的情况下，攻击者可能会产生更大的影响，因为攻击者可以假冒服务器托管的另一个域中的用户，而走私邮件的SPF检查仍会通过。

拒绝包含纯CR或LF字符的邮件

此配置选项严格强制遵守RFC。包含纯CR或LF字符的所有邮件均会被拒绝。

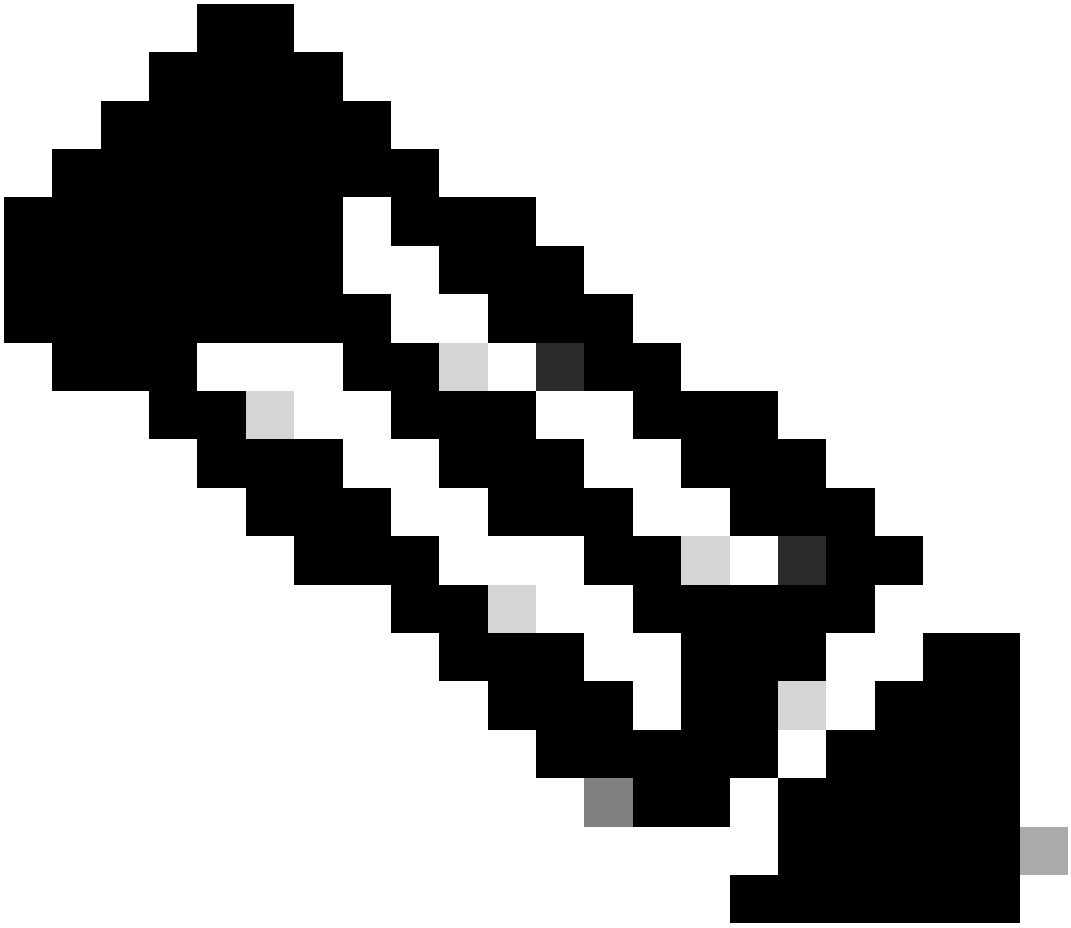


注意：虽然此配置可防止走私情况，但它也会导致来自不符合RFC标准的服务器的合法电子邮件被丢弃。

允许仅包含纯CR或LF字符的邮件（不建议使用）

最终配置导致Cisco Secure Mail使用其ASCII含义处理裸CR和LF字符。邮件正文按原样传送，包括走私内容。

由于走私邮件被视为正文的一部分，思科安全邮件可能无法检测到作为走私邮件一部分的附件。这可能会导致下游设备出现安全问题。



注意：此选项已弃用，不应再使用。

推荐 的 配置

Cisco建议使用默认的“Clean messages of bare CR and LF characters”（正常邮件的CR和LF字符数）选项，因为它在安全性和互操作性之间提供了最佳折衷。但是，使用此设置的客户应了解与走私内容相关的安全影响。希望实施RFC合规性的客户应选择“拒绝具有纯CR或LF字符的邮件”，同时注意潜在的互操作性问题。

无论如何，思科强烈建议配置和使用SPF、DomainKeys识别邮件(DKIM)或DMARC等功能来验证传入邮件的发件人。

AsyncOS版本15.0.2和15.5.1及更高版本添加了新功能，可帮助识别和过滤不符合邮件结尾RFC标准的邮件。如果接收到具有无效消息结尾顺序的消息，邮件网关会向连接内的所有消息ID (MID)添加X-Ironport-Invalid-End-Of-Message Extension Header (X-Header)，直到接收到符合消息结尾RFC标准的消息。客户可以使用内容过滤器查找“X-Ironport-Invalid-End-Of-Message”信头并定义要为这些邮件采取的操作。

常见问题解答

Cisco Secure Mail是否容易遭受上述攻击？

从技术上说，是的。当邮件中包含纯CR和LF字符时，可能导致将部分邮件作为第二封邮件处理。但是，由于第二个电子邮件是独立分析的，因此其行为等同于发送两个单独的邮件。思科未发现任何证据，表明本文所述的攻击可用于绕过任何已配置的安全过滤器。

本文提供了绕过SPF和DKIM检查的示例。为什么思科说没有绕过任何过滤器？

在这些示例中，SPF检查按预期运行，但由于发送服务器拥有多个域，因此检查通过。

建议的配置是什么？

对于客户而言，最适当的选择取决于其特定需求。建议的选项为默认的“Clean”配置或“Reject”替代配置。

选择“拒绝”选项是否会导致误报？

“拒绝”功能可启动对电子邮件是否符合RFC标准的评估。如果邮件不符合RFC标准，则会被拒绝。如果邮件不符合RFC标准，甚至合法邮件也可能会被拒绝。

是否存在涵盖此问题的软件Bug？

报告了Cisco Bug ID CSCwh10142。

如何获得有关此主题的更多信息？

任何后续问题都可以通过技术支持中心(TAC)案例提出。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。