Réponse au rapport de vulnérabilité de la passerelle de messagerie sécurisée Cisco contre la contrebande SMTP

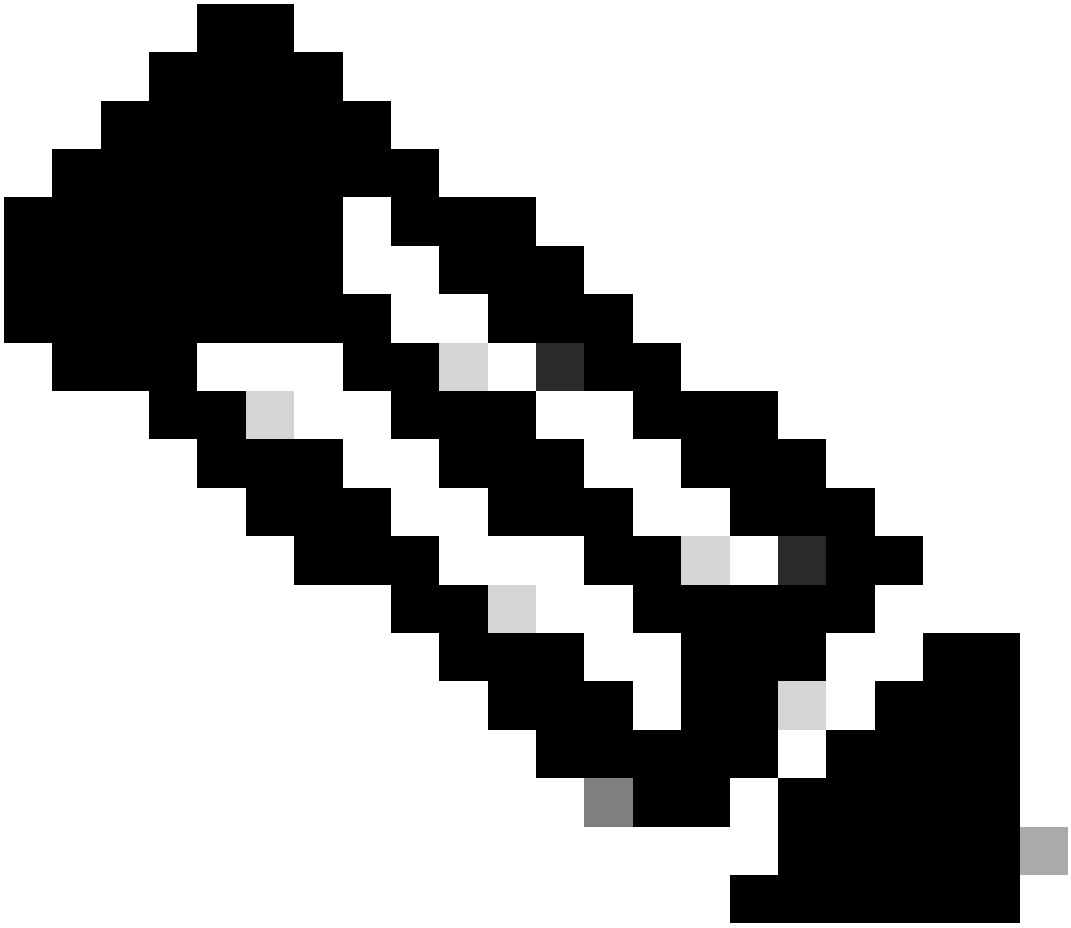
Table des matières

Introduction

Ce document fournit plus de détails sur la façon dont Cisco Secure Email se comporte par rapport au type d'attaque décrit dans SMTP Smuggling - Spoofing E-Mails Worldwide, publié le 18 décembre 2023 par SEC Consult.

Informations générales

Dans le cadre d'un projet de recherche en collaboration avec le laboratoire de vulnérabilité SEC Consult, Timo Longin (@timolongin) a découvert une nouvelle technique d'exploitation pour un autre protocole Internet - SMTP (Simple Mail Transfer Protocol). Les hameçonneurs peuvent utiliser des serveurs SMTP vulnérables dans le monde entier pour envoyer des e-mails malveillants à partir d'adresses e-mail arbitraires, ce qui permet des attaques d'hameçonnage ciblées. En raison de la nature de l'exploit lui-même, ce type de vulnérabilité a été appelé trafic SMTP.



Remarque : Cisco n'a trouvé aucune preuve que l'attaque décrite dans le document puisse être utilisée pour contourner l'un des filtres de sécurité configurés.

Contexte technique

Sans entrer dans les détails du protocole SMTP et du format de message, il est important de consulter quelques sections de la RFC 5322 afin d'obtenir du contexte.

La section 2.1 définit la séquence de caractères CRLF comme le séparateur à utiliser entre les différentes sections du message.

Les messages sont divisés en lignes de caractères. Une ligne est une série de caractères délimitée par les deux caractères retour chariot et saut de ligne, c'est-à-dire le caractère retour chariot (CR) (valeur ASCII 13) suivi immédiatement du caractère saut de ligne (LF) (valeur ASCII 10). (La paire retour chariot/saut de ligne est généralement écrite dans ce document sous la forme « CRLF ».)

La section 2.3 est plus spécifique sur le format du corps du message. Il indique clairement que les caractères CR et LF ne doivent jamais être envoyés indépendamment en tant que partie du corps. Tout serveur qui procède ainsi n'est pas conforme à la RFC.

Le corps d'un message est simplement constitué de lignes de caractères US-ASCII. Les deux seules limitations du corps sont les suivantes :

- CR et LF NE DOIVENT se produire ensemble que sous forme de CRLF ; ils NE DOIVENT PAS apparaître indépendamment dans le corps.
- Les lignes de caractères dans le corps DOIVENT être limitées à 998 caractères et doivent être limitées à 78 caractères, à l'exclusion du CRLF.

Cependant, la Section 4.1 de ce même document, à propos de la syntaxe obsolète des précédentes révisions de la RFC qui n'étaient pas aussi restrictives, reconnaît que de nombreuses implémentations sur le terrain n'utilisent pas la bonne syntaxe.

Les expressions CR et LF nues apparaissent dans des messages avec deux significations différentes. Dans de nombreux cas, la CR nue ou la LF nue sont utilisées de manière incorrecte à la place de la LF nue pour indiquer les séparateurs de ligne. Dans d'autres cas, les caractères CR et LF nus sont utilisés simplement comme caractères de contrôle US-ASCII avec leur signification ASCII traditionnelle.

Pour résumer, selon la RFC 5322, un message SMTP correctement formaté ressemblerait à ceci :

```
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
```

Le document tente de tirer parti de l'exception mentionnée à la Section 4.1 du RFC pour insérer ou « faire passer en contrebande » un nouveau message dans le corps afin de contourner les mesures de sécurité sur le serveur émetteur ou récepteur. L'objectif est que le message en contrebande contourne les contrôles de sécurité, car ces contrôles ne seraient exécutés que sur la partie du message avant que la ligne nue ne soit alimentée. Exemple :

<#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

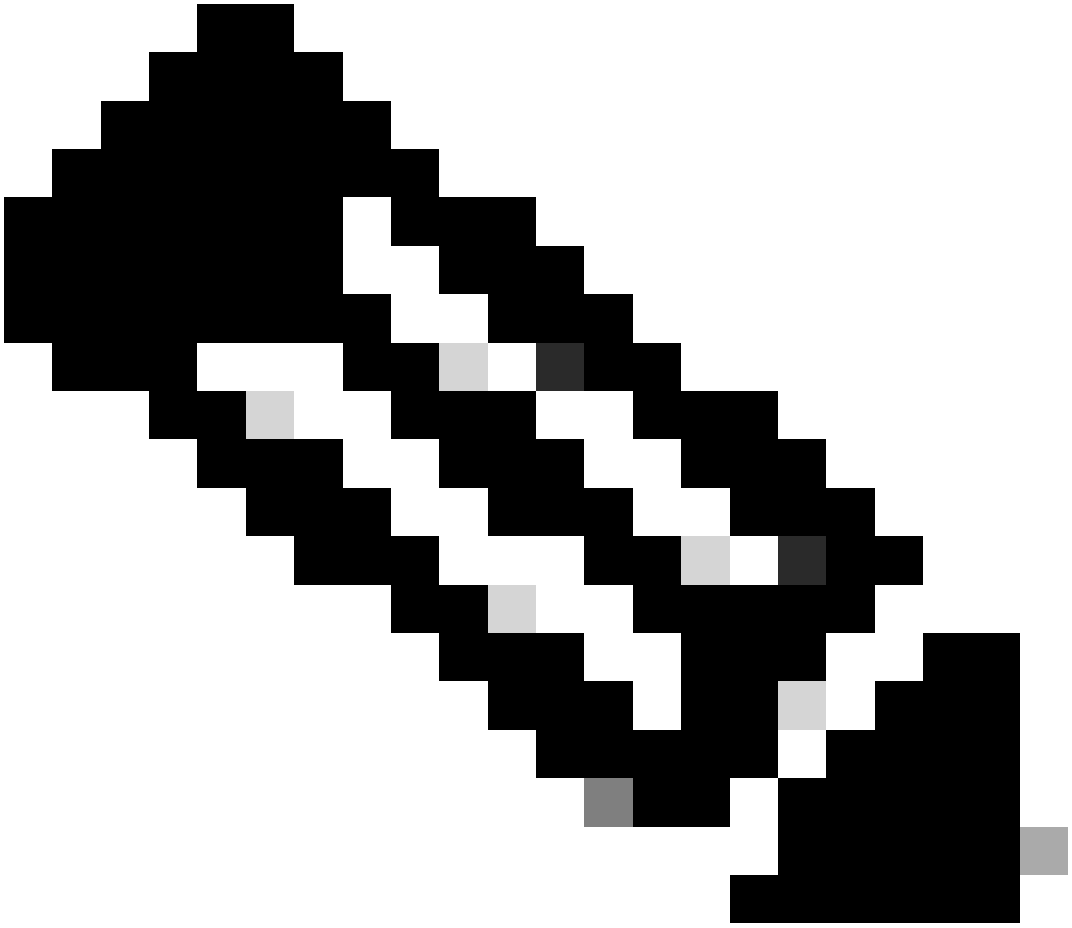
Comportement de Cisco Secure Mail

Lors de la configuration d'un écouteur SMTP sur Cisco Secure Mail, trois options de configuration déterminent la façon dont les caractères CR et LF doivent être traités.

Nettoyer les messages contenant des caractères CR et LF nus (par défaut)

Lorsque l'option par défaut est sélectionnée, Cisco Secure Mail remplace tous les caractères CR et LF nus dans les messages entrants par la séquence CRLF correcte.

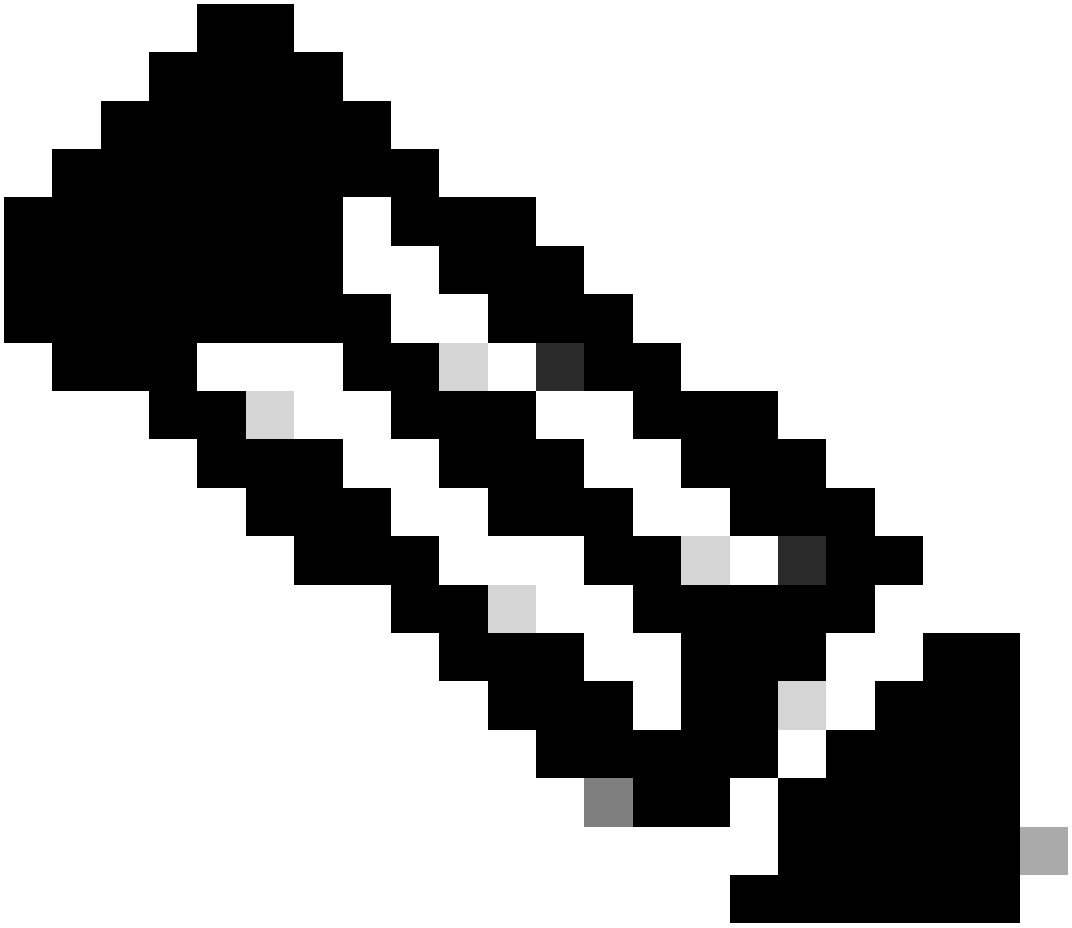
Un message dont le contenu est contrefait, comme celui de l'exemple, est traité comme deux messages distincts, et toutes les vérifications de sécurité (telles que SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication, Reporting & Conformance), AntiSpam, Antivirus, AMP (Advanced Malware Protection) et filtres de contenu) sont exécutées indépendamment sur chacun d'eux.



Remarque : les clients doivent savoir qu'avec cette configuration, un pirate peut être en mesure de faire passer un message par un autre utilisateur. Un pirate peut avoir un impact plus important dans les situations où le serveur d'origine héberge plusieurs domaines parce que le pirate peut usurper l'identité d'un utilisateur à partir de l'un des autres domaines qui sont hébergés sur le serveur, et le contrôle SPF sur le courrier électronique contrefait serait toujours réussi.

Rejeter les messages avec des caractères CR ou LF nus

Cette option de configuration applique strictement la conformité à la RFC. Tous les messages contenant des caractères CR ou LF sont rejetés.

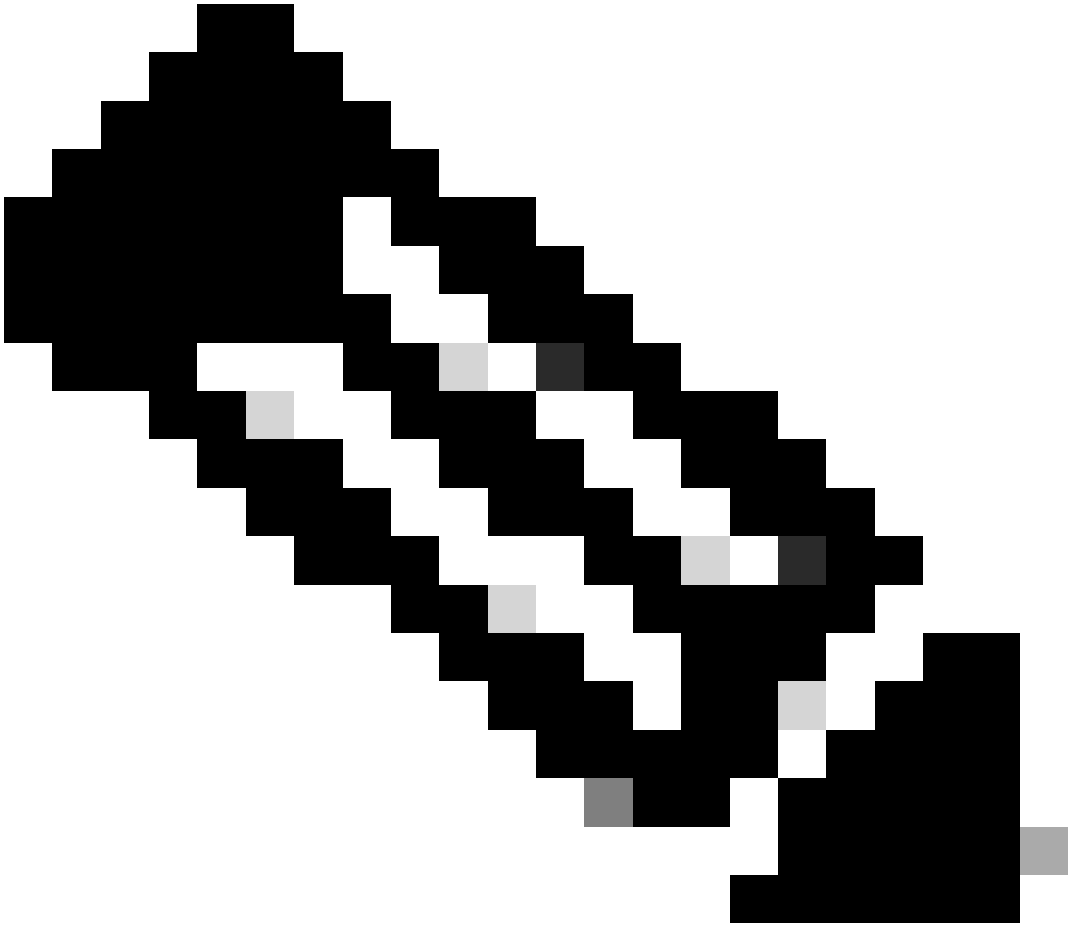


Remarque : bien que cette configuration empêche le scénario de contrebande, elle entraînera également l'abandon des e-mails légitimes provenant de serveurs qui ne sont pas conformes aux RFC.

Autoriser les messages avec caractères CR ou LF nus (déconseillé)

La configuration finale permet à Cisco Secure Mail de traiter les caractères CR et LF nus avec leur signification ASCII. Le corps du message est livré tel quel, y compris le contenu contrefait.

Étant donné que le message de contrebande est considéré comme faisant partie du corps, les pièces jointes incluses dans le message de contrebande peuvent ne pas être détectées par Cisco Secure Mail. Cela peut entraîner des problèmes de sécurité sur les périphériques en aval.



Remarque : cette option est déconseillée et ne doit plus être utilisée.

Configuration recommandée

Cisco recommande d'utiliser l'option par défaut « Nettoyer les messages de caractères CR et LF nus », car elle offre le meilleur compromis entre sécurité et interopérabilité. Toutefois, les clients qui utilisent ce paramètre doivent être conscients des implications en matière de sécurité du contenu contrefait. Les clients qui souhaitent appliquer la conformité RFC doivent choisir « Rejeter les messages avec des caractères CR ou LF nus », en étant conscients des problèmes d'interopérabilité potentiels.

Dans tous les cas, Cisco recommande vivement de configurer et d'utiliser des fonctionnalités telles que SPF, DomainKeys Identified Mail (DKIM) ou DMARC pour valider l'expéditeur d'un message entrant.

AsyncOS versions 15.0.2 et 15.5.1 et ultérieures ajoute de nouvelles fonctionnalités qui permettent d'identifier et de filtrer les messages qui ne sont pas conformes à la norme RFC de fin

de message. Si un message avec une séquence de fin de message non valide est reçu, la passerelle de messagerie ajoute un en-tête d'extension X-Ironport-Invalid-End-Of-Message (X-Header) à tous les ID de message (MID) dans cette connexion jusqu'à ce qu'un message conforme à la norme RFC de fin de message soit reçu. Les clients peuvent utiliser un filtre de contenu pour rechercher l'en-tête « X-Ironport-Invalid-End-Of-Message » et définir les actions à entreprendre pour ces messages.

Forum aux questions

Cisco Secure Mail est-il vulnérable à l'attaque décrite ?

Techniquement, oui. Lorsque des caractères CR et LF nus sont inclus dans le courrier, il est possible de traiter une partie du courrier comme un deuxième courrier électronique. Cependant, comme le deuxième e-mail est analysé indépendamment, le comportement équivaut à envoyer deux messages distincts. Cisco n'a trouvé aucune preuve que l'attaque décrite dans le document pourrait être utilisée pour contourner l'un des filtres de sécurité configurés.

Le document fournit des exemples de contrôles SPF et DKIM contournés. Pourquoi Cisco dit-il qu'aucun filtre n'est contourné ?

Dans ces exemples, les vérifications SPF sont exécutées comme prévu, mais aboutissent à une vérification réussie en raison du fait que le serveur émetteur possède plusieurs domaines.

Quelle est la configuration recommandée ?

Le choix le plus approprié pour un client dépend de ses besoins spécifiques. Les options recommandées sont soit la configuration par défaut "Nettoyer" ou l'alternative "Rejeter".

Le choix de l'option Rejeter entraînera-t-il des faux positifs ?

La fonction « Rejeter » lance une évaluation de la conformité de l'e-mail aux normes RFC. Si l'e-mail n'est pas conforme aux normes RFC, il sera refusé. Même les e-mails légitimes peuvent être rejetés si l'e-mail n'est pas conforme aux normes RFC.

Y a-t-il un bogue logiciel qui couvre ce problème ?

L'ID de bogue Cisco CSCwh10142 a été classé.

Comment puis-je obtenir plus d'informations sur ce sujet ?

Toutes les questions de suivi peuvent être posées par le biais d'un dossier du Centre d'assistance technique (TAC).

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.