Risposta al report sulle vulnerabilità del contrabbando SMTP di Cisco Secure Email Gateway

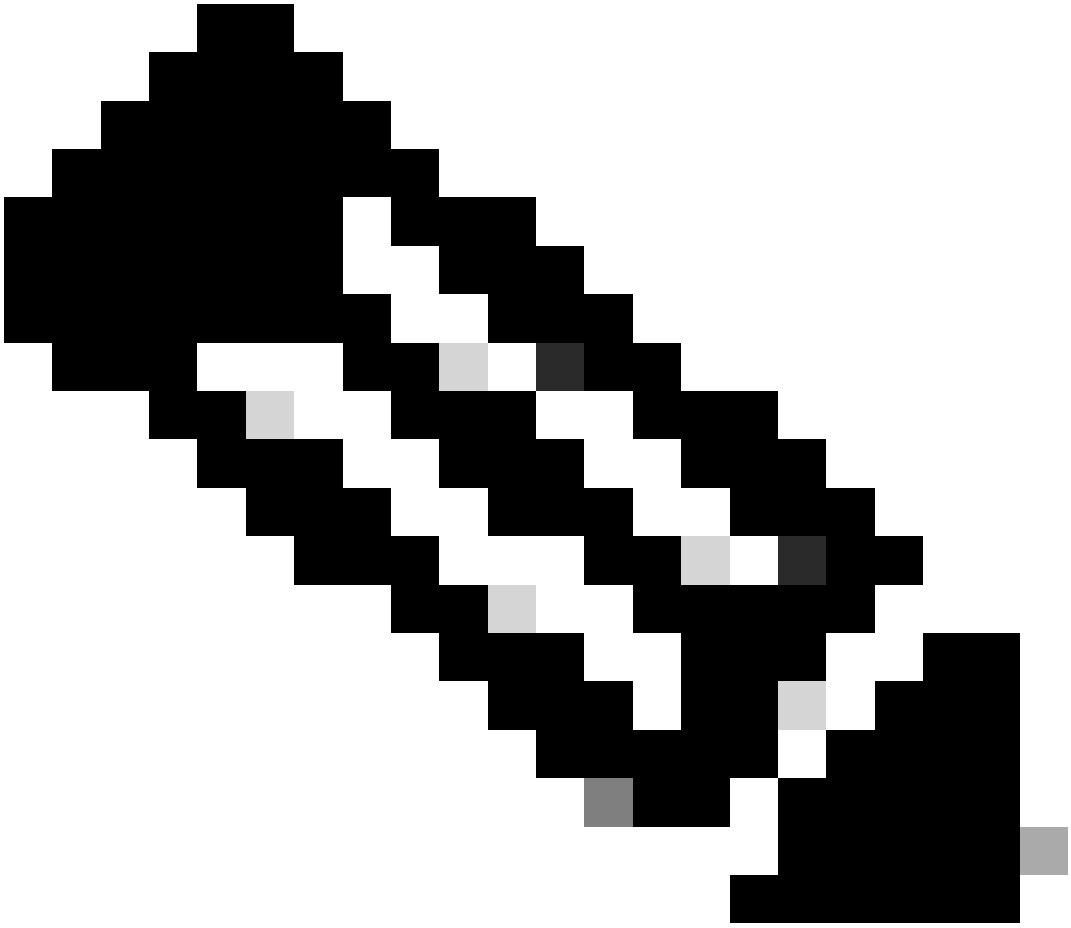
Sommario

Introduzione

Questo documento offre ulteriori dettagli su come Cisco Secure Email si comporta contro il tipo di attacco descritto in SMTP Contrabbando - Spoofing E-Mail Worldwide, pubblicato il 18 dicembre 2023 da SEC Consult.

Premesse

Nel corso di un progetto di ricerca in collaborazione con il laboratorio di vulnerabilità della SEC Consult, Timo Longin (@timolongin) ha scoperto una nuova tecnica di sfruttamento per l'ennesimo protocollo Internet - SMTP (Simple Mail Transfer Protocol). Gli attori della minaccia potrebbero abusare dei server SMTP vulnerabili in tutto il mondo per inviare e-mail dannose da indirizzi e-mail arbitrari, consentendo attacchi mirati di phishing. A causa della natura stessa dell'exploit, questo tipo di vulnerabilità è stato soprannominato contrabbando SMTP.



Nota: Cisco non ha trovato alcuna prova che l'attacco descritto nel documento possa essere usato per bypassare uno qualsiasi dei filtri di sicurezza configurati.

Contesto tecnico

Senza entrare nei dettagli sul protocollo SMTP e sul formato dei messaggi, è importante esaminare alcune sezioni della RFC 5322 per ottenere informazioni sul contesto.

La sezione 2.1 definisce la sequenza di caratteri CRLF come il separatore da utilizzare tra le diverse sezioni del messaggio.

I messaggi sono divisi in righe di caratteri. Una riga è una serie di caratteri delimitati da due caratteri di ritorno a capo e avanzamento riga, ovvero il carattere di ritorno a capo (CR) (valore ASCII 13) seguito immediatamente dal carattere di avanzamento riga (LF) (valore ASCII 10). (la coppia ritorno a capo/avanzamento riga è generalmente scritta in questo documento come "CRLF").

La sezione 2.3 è più specifica sul formato del corpo del messaggio. Stabilisce chiaramente che i caratteri CR e LF non devono mai essere inviati in modo indipendente come parte del corpo. Qualsiasi server che esegua questa operazione non è conforme alla RFC.

Il corpo di un messaggio è costituito semplicemente da righe di caratteri US-ASCII. Le uniche due limitazioni del corpo sono le seguenti:

- CR e LF DEVONO trovarsi solo insieme come CRLF; NON DEVONO apparire in modo indipendente nel corpo.
- Le righe di caratteri nel corpo DEVONO essere limitate a 998 caratteri e a 78 caratteri, escluso il CRLF.

Tuttavia, la sezione 4.1 dello stesso documento, relativa alla sintassi obsoleta di precedenti revisioni della RFC che non erano così restrittive, riconosce che molte implementazioni sul campo non utilizzano la sintassi corretta.

I termini CR e LF nudi vengono visualizzati nei messaggi con due significati diversi. In molti casi, per indicare i separatori di riga vengono utilizzati in modo non corretto i filtri CR o LF nudi anziché i filtri CRLF. In altri casi, i caratteri CR e LF nudi vengono utilizzati semplicemente come caratteri di controllo US-ASCII con i loro significati ASCII tradizionali.

Per riepilogare, in base alla RFC 5322, un messaggio SMTP formattato correttamente avrebbe il seguente aspetto:

```
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
```

Il documento tenta di sfruttare l'eccezione menzionata nella Sezione 4.1 della RFC per inserire o "contrabbandare" un nuovo messaggio come parte del corpo nel tentativo di eludere le misure di sicurezza sul server di invio o di ricezione. L'obiettivo è evitare che il messaggio contrabbandato esegua i controlli di sicurezza, in quanto tali controlli verrebbero eseguiti solo sulla parte del messaggio precedente all'avanzamento riga. Ad esempio:

<#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
```

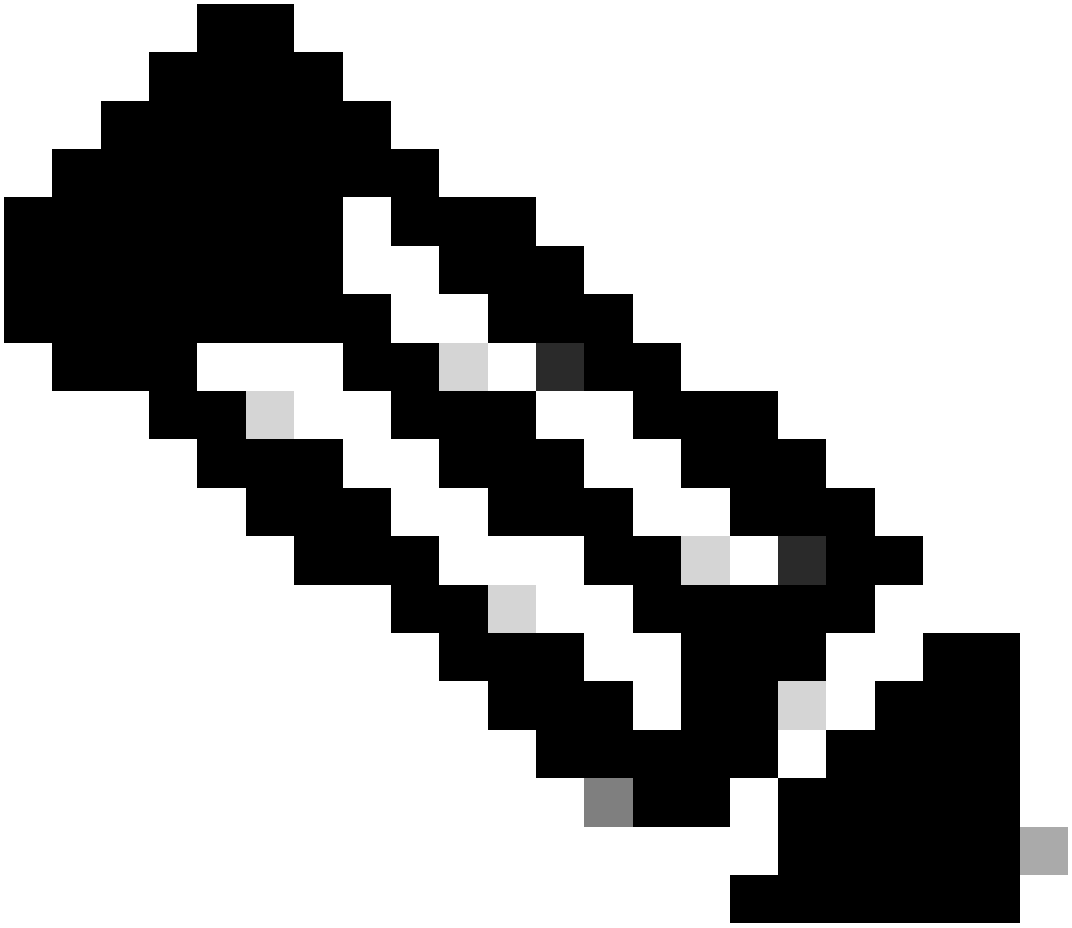
Comportamento di Cisco Secure Mail

Quando si configura un listener SMTP in Cisco Secure Mail, tre opzioni di configurazione determinano il modo in cui devono essere trattati i caratteri CR e LF nudi.

Messaggi puliti di caratteri CR e LF non significativi (impostazione predefinita)

Se l'opzione predefinita è selezionata, Cisco Secure Mail sostituisce tutti i caratteri CR e LF non selezionati nei messaggi in arrivo con la sequenza CRLF corretta.

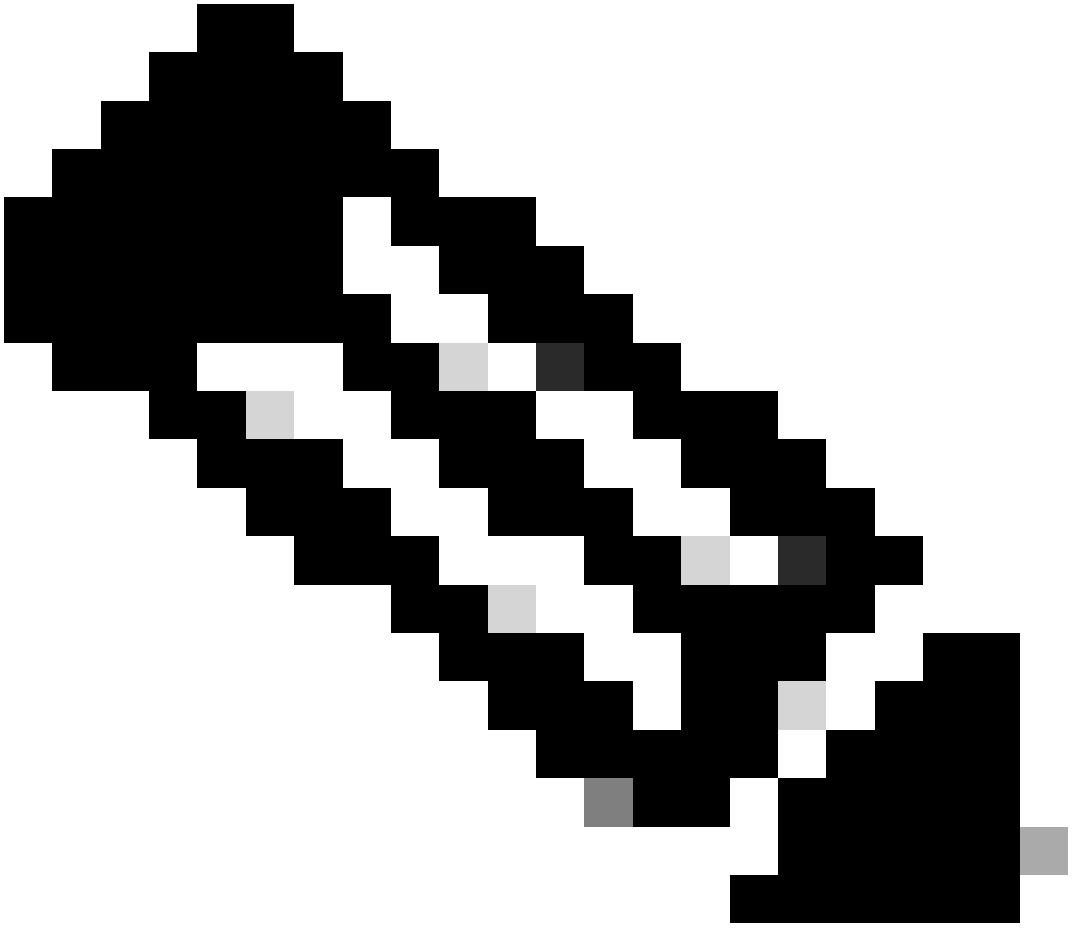
Un messaggio con contenuto di contrabbando, come quello dell'esempio, viene trattato come due messaggi distinti e tutti i controlli di sicurezza (come Sender Policy Framework (SPF), Domain-based Message Authentication, Reporting & Conformance (DMARC), AntiSpam, Antivirus, Advanced Malware Protection (AMP) e i filtri contenuti) vengono eseguiti in modo indipendente su ciascuno di essi.



Nota: i clienti devono essere consapevoli che, con questa configurazione, un utente malintenzionato potrebbe essere in grado di contrabbandare un messaggio che rappresenta un altro utente. Un utente malintenzionato potrebbe avere un impatto maggiore in situazioni in cui il server di origine ospita più domini, in quanto l'utente malintenzionato potrebbe rappresentare un utente di uno degli altri domini ospitati sul server e il controllo SPF sull'e-mail contrabbandata sarebbe comunque riuscito.

Rifiuta messaggi con caratteri CR o LF vuoti

Questa opzione di configurazione garantisce la conformità con l'RFC. Tutti i messaggi contenenti caratteri CR o LF nudi vengono rifiutati.

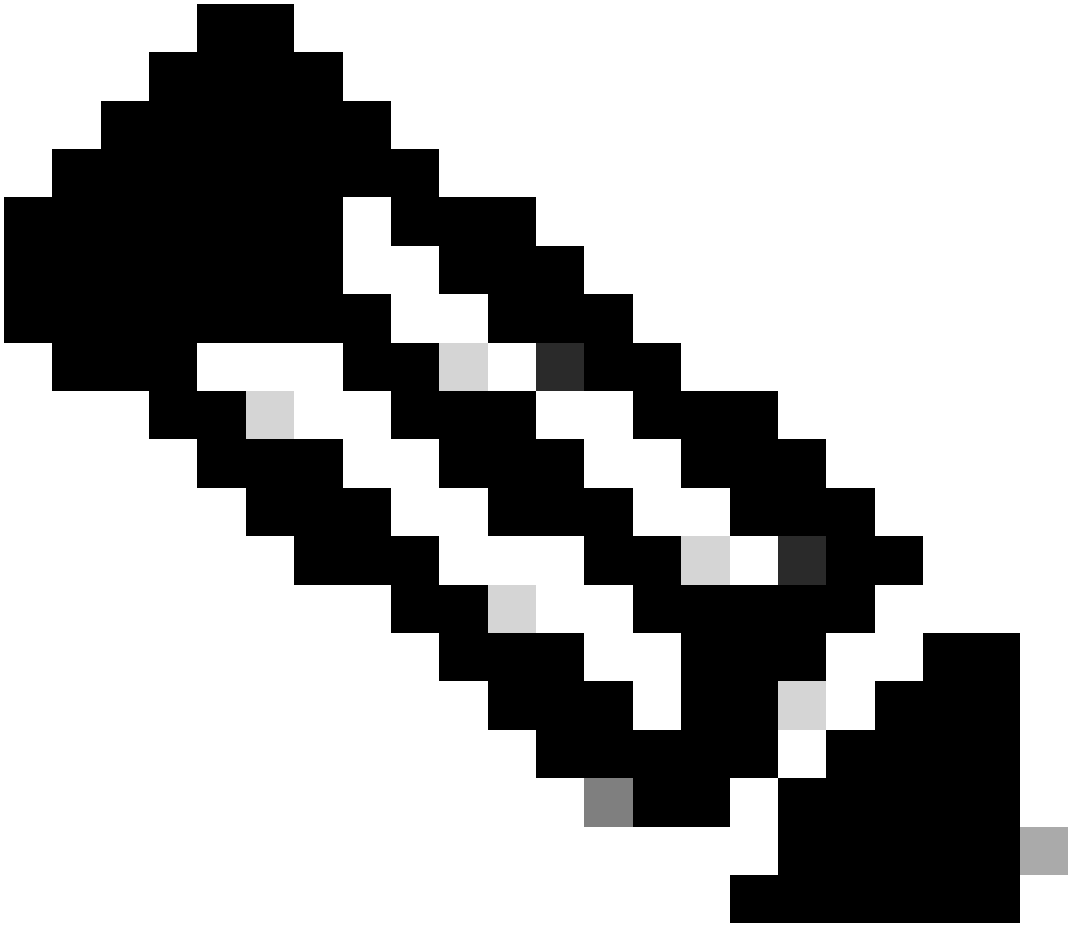


Nota: anche se questa configurazione impedisce lo scenario di contrabbando, causerà anche l'eliminazione delle e-mail legittime provenienti da server non conformi alla RFC.

Consenti messaggi con caratteri CR o LF non significativi (deprecati)

Nella configurazione finale, Cisco Secure Mail considera i caratteri CR e LF nudi con il loro significato ASCII. Il corpo del messaggio viene consegnato così com'è, inclusi i contenuti contrabbandati.

Poiché il messaggio contrabbandato viene trattato come parte del corpo, gli allegati inclusi come parte del messaggio contrabbandato potrebbero non essere rilevati da Cisco Secure Mail. Ciò potrebbe causare problemi di sicurezza nei dispositivi downstream.



Nota: questa opzione è obsoleta e non deve più essere utilizzata.

Configurazione consigliata

Cisco consiglia di utilizzare l'opzione predefinita "Clean messages of bare CR and LF characters" (Messaggi puliti di caratteri CR e LF nudi), in quanto offre il miglior compromesso tra sicurezza e interoperabilità. Tuttavia, i clienti che utilizzano questa impostazione devono essere consapevoli delle implicazioni di sicurezza per quanto riguarda i contenuti di contrabbando. I clienti che desiderano applicare la conformità RFC devono scegliere "Rifiuta i messaggi con caratteri CR o LF nudi", tenendo presente i potenziali problemi di interoperabilità.

In ogni caso Cisco consiglia vivamente di configurare e utilizzare funzionalità quali SPF, DKIM (DomainKeys Identified Mail) o DMARC per convalidare il mittente di un messaggio in arrivo.

AsyncOS versione 15.0.2 e 15.5.1 e successive aggiunge una nuova funzionalità che aiuta a identificare e filtrare i messaggi che non sono conformi allo standard RFC di fine messaggio. Se viene ricevuto un messaggio con una sequenza di fine messaggio non valida, il gateway di posta

elettronica aggiunge un'intestazione X-Ironport-Invalid-End-Of-Message Extension (X-Header) a tutti gli ID messaggio (MID) all'interno della connessione finché non viene ricevuto un messaggio conforme allo standard RFC di fine messaggio. I clienti possono utilizzare un filtro contenuti per cercare l'intestazione "X-Ironport-Invalid-End-Of-Message" e definire le azioni da intraprendere per questi messaggi.

Domande frequenti

Cisco Secure Mail è vulnerabile all'attacco descritto?

Tecnicamente, sì. Se nella posta sono inclusi i caratteri CR e LF non codificati, è possibile che parte dell'e-mail venga trattata come una seconda e-mail. Tuttavia, poiché la seconda e-mail viene analizzata in modo indipendente, il comportamento equivale all'invio di due messaggi separati. Cisco non ha trovato alcuna prova che l'attacco descritto nel documento possa essere usato per bypassare uno qualsiasi dei filtri di sicurezza configurati.

In questo documento vengono illustrati alcuni esempi di controlli SPF e DKIM ignorati. Perché Cisco dice che non si stanno ignorando i filtri?

In questi esempi, i controlli SPF vengono eseguiti come previsto, ma il risultato è un controllo superato, in quanto il server di invio è proprietario di più domini.

Qual è la configurazione consigliata?

La scelta più appropriata per un cliente dipende dalle sue esigenze specifiche. Le opzioni consigliate sono la configurazione "Pulisci" predefinita o l'alternativa "Rifiuta".

La scelta dell'opzione Rifiuta darà luogo a falsi positivi?

La funzione "Reject" (Rifiuta) avvia una valutazione della conformità dell'e-mail agli standard RFC. Se l'e-mail non è conforme agli standard RFC, verrà rifiutata. Anche le e-mail legittime possono essere rifiutate se non sono conformi agli standard RFC.

Il problema è stato risolto con un bug software?

L'ID bug Cisco CSCwh10142 è stato archiviato.

Come ottenere ulteriori informazioni su questo argomento?

Eventuali domande di follow-up possono essere presentate tramite un caso TAC (Technical

Assistance Center).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).