Respuesta al informe de vulnerabilidad de contrabando de SMTP de Cisco Secure Email Gateway

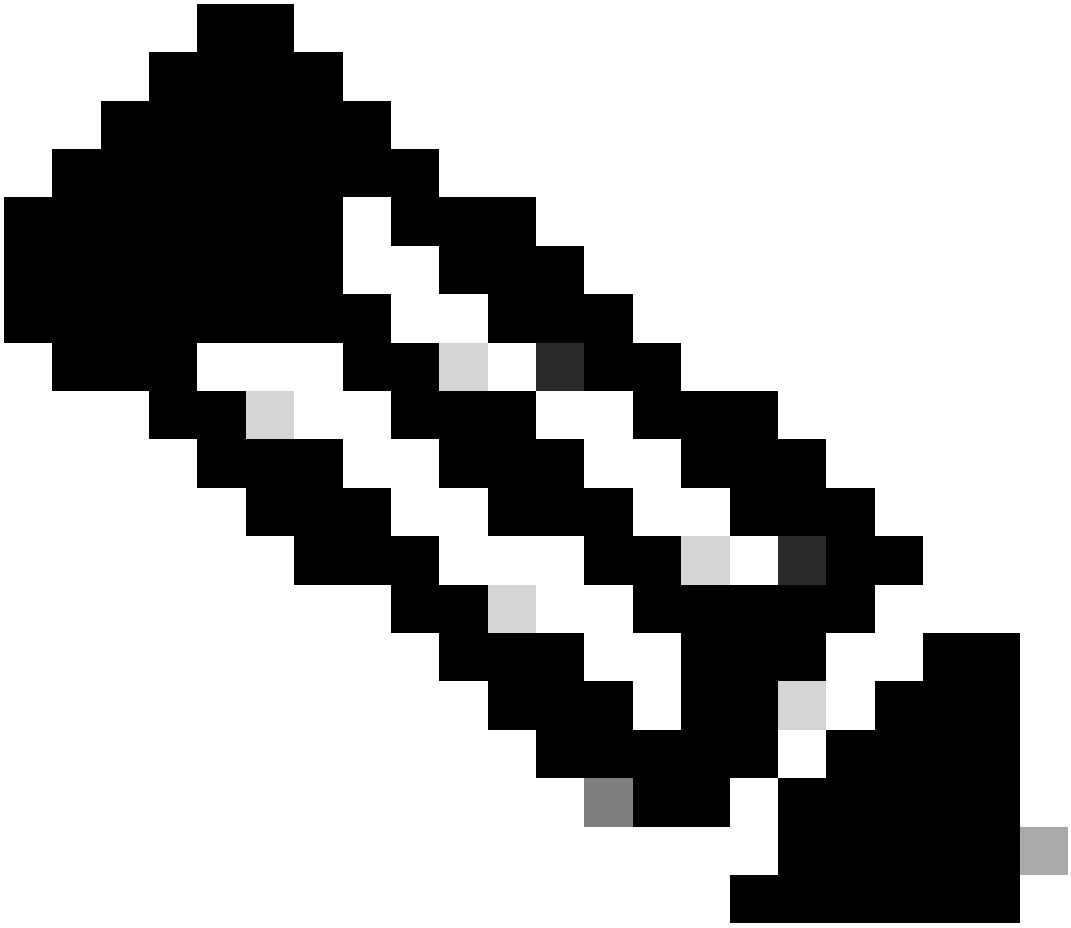
Contenido

Introducción

Este documento proporciona más detalles sobre cómo se comporta Cisco Secure Email frente al tipo de ataque descrito en SMTP Smuggling - Spoofing E-Mails Worldwide, publicado el 18 de diciembre de 2023 por SEC Consult.

Antecedentes

En el curso de un proyecto de investigación en colaboración con el Laboratorio de Vulnerabilidad de SEC Consult, Timo Longin (@timolongin) descubrió una novedosa técnica de explotación para otro protocolo de Internet - SMTP (Simple Mail Transfer Protocol). Los agentes de amenazas podrían abusar de servidores SMTP vulnerables de todo el mundo para enviar correos electrónicos maliciosos desde direcciones de correo electrónico arbitrarias, lo que permitiría ataques de phishing dirigidos. Debido a la naturaleza de la vulnerabilidad en sí, este tipo de vulnerabilidad se denominó contrabando de SMTP.



Nota: Cisco no ha encontrado ninguna prueba de que el ataque descrito en el informe pueda utilizarse para omitir ninguno de los filtros de seguridad configurados.

Antecedentes técnicos

Sin entrar en detalles sobre el protocolo SMTP y el formato del mensaje, es importante observar algunas secciones de RFC 5322 para obtener algún contexto.

La sección 2.1 define la secuencia de caracteres CRLF como el separador que se utilizará entre las diferentes secciones del mensaje.

Los mensajes se dividen en líneas de caracteres. Una línea es una serie de caracteres delimitados por los caracteres retorno de carro y salto de línea, es decir, el carácter de retorno de carro (CR) (valor ASCII 13) seguido inmediatamente por el carácter de salto de línea (LF) (valor ASCII 10). (El par retorno de carro/avance de línea se suele escribir en este documento como "CRLF".)

La sección 2.3 es más específica sobre el formato del cuerpo del mensaje. Establece claramente que los caracteres CR y LF nunca deben enviarse de forma independiente como parte del cuerpo. Cualquier servidor que lo haga no cumple con el RFC.

El cuerpo de un mensaje es simplemente líneas de caracteres US-ASCII. Las únicas dos limitaciones en el cuerpo son las siguientes:

- CR y LF SOLO DEBEN aparecer juntos como CRLF; NO DEBEN aparecer independientemente en el cuerpo.
- Las líneas de caracteres del cuerpo DEBEN limitarse a 998 caracteres y a 78 caracteres, excluido el CRLF.

Sin embargo, la Sección 4.1 de ese mismo documento, sobre la sintaxis obsoleta de revisiones anteriores de RFC que no eran tan restrictivas, reconoce que muchas implementaciones en el campo no están usando la sintaxis correcta.

La CR simple y la LF simple aparecen en mensajes con dos significados diferentes. En muchos casos, se utiliza CR desnudo o LF desnudo incorrectamente en lugar de CRLF para indicar separadores de línea. En otros casos, CR simple y LF simple se utilizan simplemente como caracteres de control US-ASCII con sus significados ASCII tradicionales.

En resumen, según RFC 5322, un mensaje SMTP con formato correcto tendría este aspecto:

```
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
```

El documento intenta aprovechar la excepción mencionada en la Sección 4.1 del RFC para insertar o "pasar de contrabando" un nuevo mensaje como parte del cuerpo en un intento de eludir las medidas de seguridad en el servidor de envío o recepción. El objetivo es que el mensaje de contrabando pase por alto las comprobaciones de seguridad, ya que estas comprobaciones sólo se ejecutarían en la parte del mensaje antes de que la línea vacía se alimente. Por ejemplo:

<#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
```

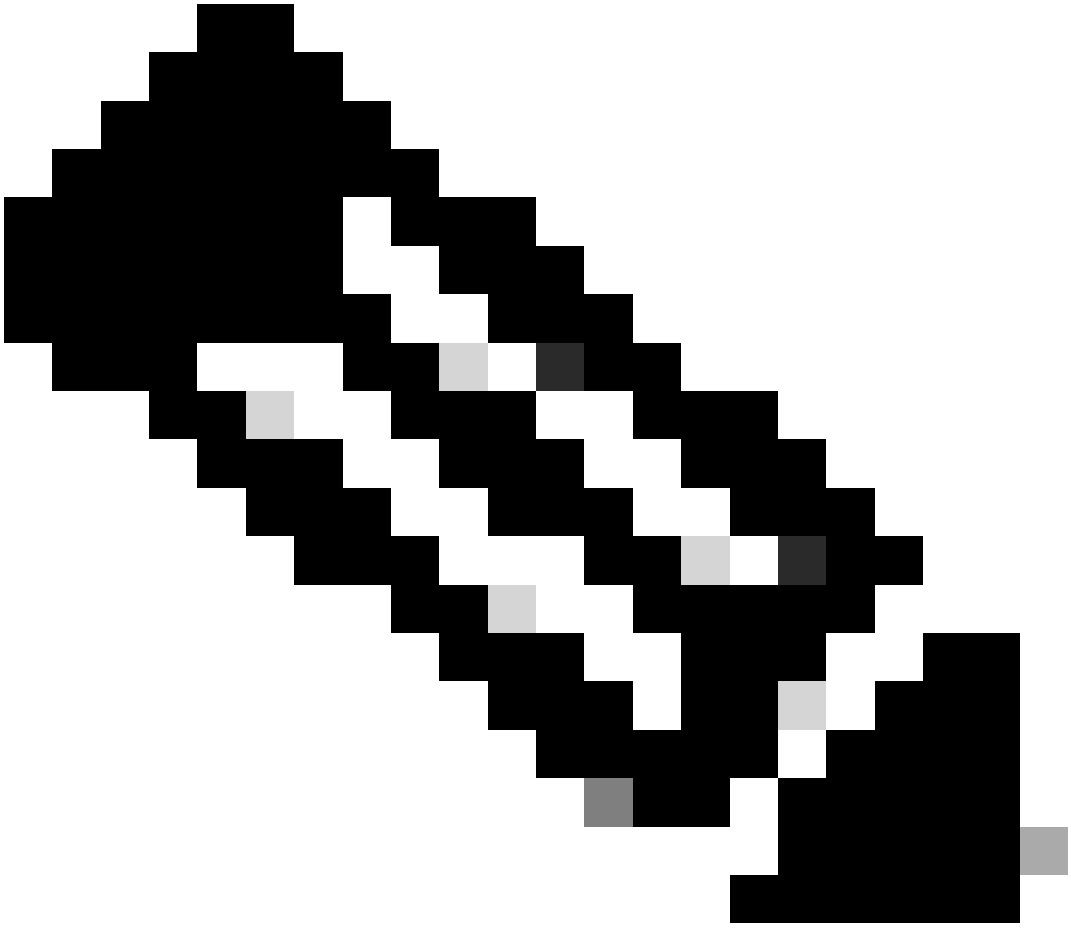
Comportamiento de Cisco Secure Mail

Al configurar un receptor SMTP en Cisco Secure Mail, tres opciones de configuración determinan cómo deben tratarse los caracteres CR y LF simples.

Limpiar mensajes de caracteres CR y LF simples (predeterminado)

Con la opción predeterminada seleccionada, Cisco Secure Mail sustituye todos los caracteres CR y LF simples de los mensajes entrantes por la secuencia CRLF correcta.

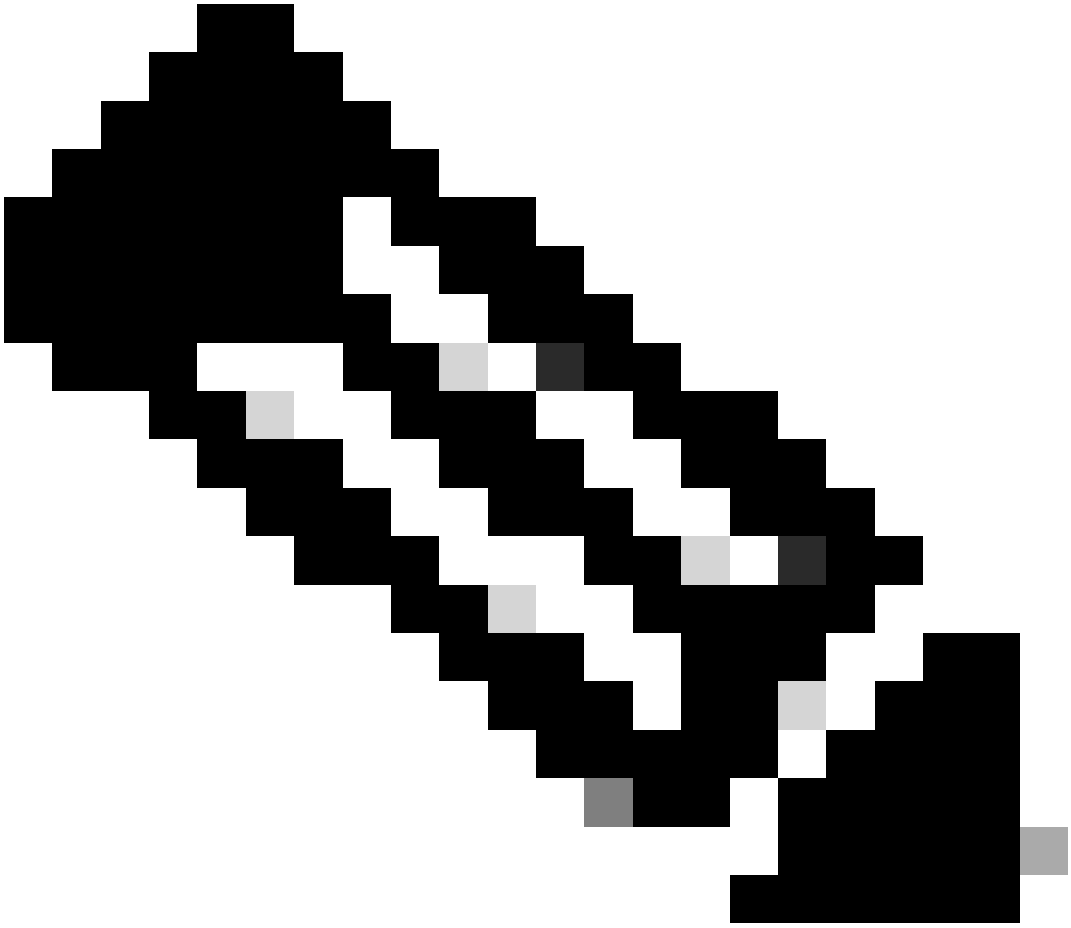
Un mensaje con contenido de contrabando, como el del ejemplo, se trata como dos mensajes independientes, y todas las comprobaciones de seguridad (como el marco de políticas de remitentes (SPF), la autenticación de mensajes basada en dominio, la generación de informes y conformidad (DMARC), antispam, antivirus, protección frente a malware avanzado (AMP) y filtros de contenido) se ejecutan de forma independiente en cada uno de ellos.



Nota: los clientes deben tener en cuenta que, con esta configuración, un atacante podría pasar de contrabando un mensaje que suplantara a otro usuario. Un atacante podría tener un mayor impacto en situaciones en las que el servidor de origen aloja varios dominios porque podría suplantar a un usuario de uno de los otros dominios alojados en el servidor, y la verificación SPF en el correo electrónico de contrabando seguiría pasando.

Rechazar mensajes con caracteres CR o LF simples

Esta opción de configuración aplica estrictamente el cumplimiento de RFC. Los mensajes que contengan caracteres CR o LF simples se rechazarán.

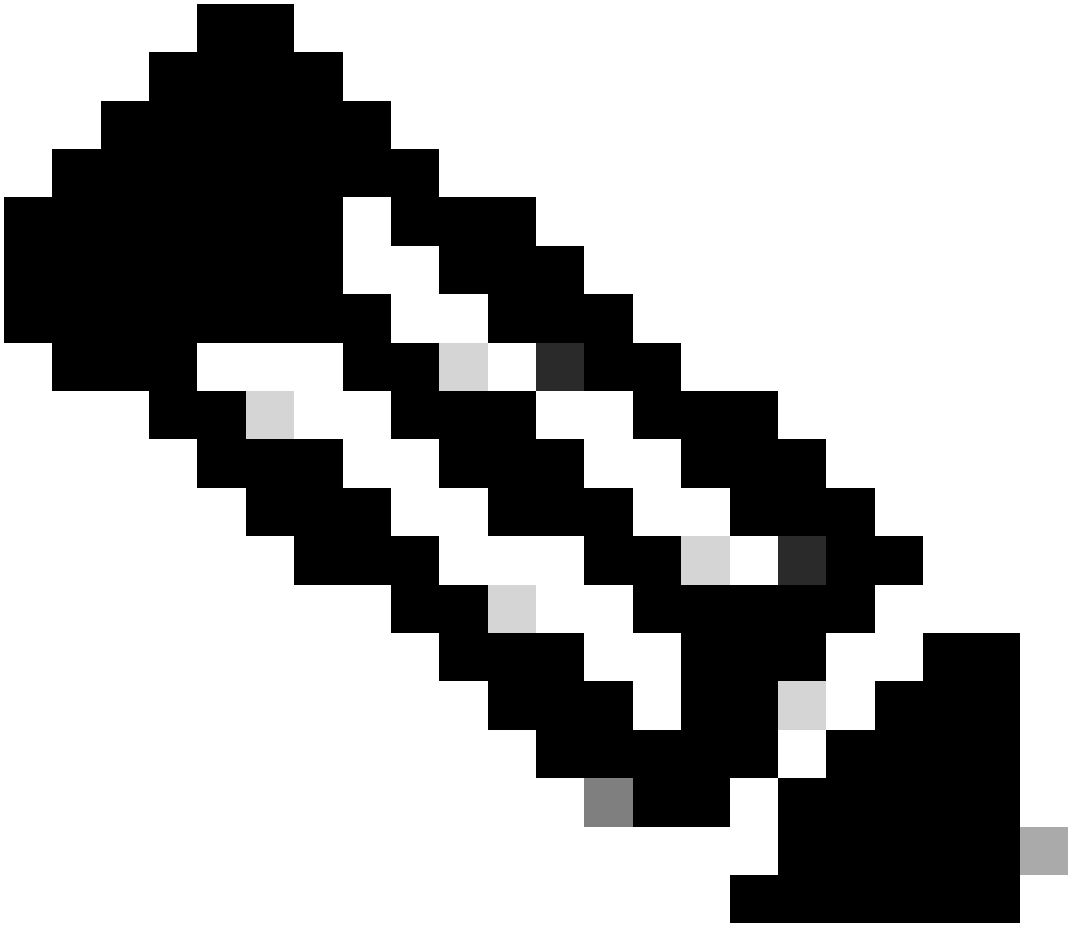


Nota: aunque esta configuración evita el escenario de contrabando, también hará que se descarten los correos electrónicos legítimos provenientes de servidores que no cumplen con RFC.

Permitir mensajes con caracteres CR o LF simples (obsoletos)

La configuración final hace que Cisco Secure Mail trate los caracteres CR y LF sin formato con su significado ASCII. El cuerpo del mensaje se entrega tal cual, incluido el contenido de contrabando.

Como el mensaje de contrabando se trata como parte del cuerpo, es posible que Cisco Secure Mail no detecte los archivos adjuntos incluidos como parte del mensaje de contrabando. Esto podría causar problemas de seguridad en los dispositivos descendentes.



Nota: Esta opción ha quedado obsoleta y ya no debe utilizarse.

Configuración recomendada

Cisco recomienda utilizar la opción predeterminada "Limpiar mensajes de caracteres CR y LF simples" porque ofrece el mejor riesgo entre seguridad e interoperabilidad. Sin embargo, los clientes que utilicen esta configuración deben ser conscientes de las implicaciones de seguridad con respecto al contenido de contrabando. Los clientes que deseen aplicar el cumplimiento de RFC deben elegir "Rechazar mensajes con caracteres CR o LF simples", conscientes de los posibles problemas de interoperabilidad.

En cualquier caso, Cisco recomienda encarecidamente configurar y utilizar funciones como SPF, DomainKeys Identified Mail (DKIM) o DMARC para validar el remitente de un mensaje entrante.

Las versiones 15.0.2 y 15.5.1 y posteriores de AsyncOS agregan nuevas funciones que ayudan a identificar y filtrar los mensajes que no cumplen con el estándar RFC de fin de mensaje. Si se recibe un mensaje con una secuencia de fin de mensaje no válida, el gateway de correo

electrónico agrega un encabezado de extensión de fin de mensaje (encabezado X) X-Ironport-Invalid-End-Of-Message a todos los identificadores de mensaje (MID) de esa conexión hasta que se reciba un mensaje que cumpla con el estándar RFC de fin de mensaje. Los clientes pueden utilizar un filtro de contenido para buscar el encabezado "X-Ironport-Invalid-End-Of-Message" y definir las acciones que deben llevarse a cabo para estos mensajes.

Preguntas Frecuentes

¿Es Cisco Secure Mail vulnerable al ataque descrito?

Técnicamente, sí. Cuando se incluyen caracteres CR y LF simples en el correo, es posible hacer que parte del correo electrónico se trate como un segundo correo electrónico. Sin embargo, dado que el segundo correo electrónico se analiza de forma independiente, el comportamiento equivale a enviar dos mensajes independientes. Cisco no ha encontrado ninguna prueba de que el ataque descrito en el informe pueda utilizarse para eludir cualquiera de los filtros de seguridad configurados.

El documento proporciona ejemplos de verificaciones SPF y DKIM omitidas. ¿Por qué afirma Cisco que no se está omitiendo ningún filtro?

En estos ejemplos, las comprobaciones SPF se ejecutan según lo esperado, pero dan como resultado una comprobación superada debido a que el servidor de envío posee varios dominios.

¿Cuál es la configuración recomendada?

La opción más adecuada para un cliente depende de sus requisitos específicos. Las opciones recomendadas son la configuración "Limpiar" predeterminada o la alternativa "Rechazar".

¿La elección de la opción Rechazar dará como resultado falsos positivos?

La función "Rechazar" inicia una evaluación del cumplimiento del correo electrónico con los estándares RFC. Si el correo electrónico no cumple con los estándares RFC, se rechazará. Incluso los correos electrónicos legítimos se pueden rechazar si el correo electrónico no cumple con los estándares RFC.

¿Hay algún bug de software que cubra este problema?

El ID de bug de Cisco CSCwh10142 fue archivado.

¿Cómo puedo obtener más información sobre este tema?

Cualquier pregunta de seguimiento puede plantearse a través de un caso del Technical Assistance Center (TAC).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).