Resposta ao Relatório de Vulnerabilidade de Contrabando de SMTP do Cisco Secure Email Gateway

Contents

Introdução

Este documento fornece mais detalhes sobre como o Cisco Secure Email se comporta contra o tipo de ataque descrito em SMTP Smuggling - Spoofing E-Mails Worldwide, publicado em 18 de dezembro de 2023 pela SEC Consult.

No decorrer de um projeto de pesquisa em colaboração com o Laboratório de Vulnerabilidade da SEC Consult, Timo Longin (@timolongin) descobriu uma nova técnica de exploração para mais um protocolo de Internet - o SMTP (Simple Mail Transfer Protocol). Os agentes de ameaças podem abusar de servidores SMTP vulneráveis em todo o mundo para enviar e-mails mal-intencionados de endereços de e-mail arbitrários, permitindo ataques de phishing direcionados. Devido à natureza da exploração em si, esse tipo de vulnerabilidade foi apelidado de contrabando SMTP.

A Cisco não encontrou nenhuma evidência de que o ataque descrito no artigo pudesse ser usado para ignorar qualquer um dos filtros de segurança configurados.

Experiência técnica

Sem entrar em detalhes sobre o protocolo SMTP e o formato da mensagem, é importante examinar algumas seções do RFC 5322 para obter algum contexto.

A seção 2.1 define a sequência de caracteres CRLF como o separador a utilizar entre as diferentes seções da mensagem.

As mensagens são divididas em linhas de caracteres. Uma linha é uma série de caracteres que é delimitada com os dois caracteres de retorno de carro e alimentação de linha; isto é, o caractere

de retorno de carro (CR) (valor ASCII 13) seguido imediatamente pelo caractere de alimentação de linha (LF) (valor ASCII 10). (O par de retorno de carro/alimentação de linha é geralmente escrito neste documento como "CRLF".)

A seção 2.3 é mais específica sobre o formato do corpo da mensagem. Ele afirma claramente que os caracteres CR e LF nunca devem ser enviados independentemente como parte do corpo. Qualquer servidor que faça isso não está em conformidade com o RFC.

O corpo de uma mensagem são simplesmente linhas de caracteres US-ASCII. As duas únicas limitações no corpo são as seguintes:

- CR e LF DEVEM ocorrer em conjunto como CRLF; NÃO DEVEM aparecer de forma independente no corpo.
- As linhas de caracteres no corpo DEVEM ser limitadas a 998 caracteres e DEVEM ser limitadas a 78 caracteres, excluindo o CRLF.

No entanto, a Seção 4.1 desse mesmo documento, em referência à sintaxe obsoleta de revisões anteriores do RFC que não eram tão restritivas, reconhece que muitas implementações no campo não estão usando a sintaxe correta.

CR e LF expostos aparecem em mensagens com dois significados diferentes. Em muitos casos, CR ou LF desencapados são usados incorretamente em vez de CRLF para indicar separadores de linha. Em outros casos, CR e LF são usados simplesmente como caracteres de controle US-ASCII com seus significados ASCII tradicionais.

Para resumir, de acordo com o RFC 5322, uma mensagem SMTP formatada corretamente seria semelhante ao seguinte exemplo:

```
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
```

O papel tenta aproveitar a exceção mencionada na Seção 4.1 do RFC para inserir ou "contrabandear" uma nova mensagem como parte do corpo em uma tentativa de ignorar as medidas de segurança no servidor de envio ou de recebimento. O objetivo é que a mensagem contrabandeada ignore as verificações de segurança, pois essas verificações só seriam executadas na parte da mensagem antes que a linha pura seja alimentada. Por exemplo:

<#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 do Cisco Secure Mail

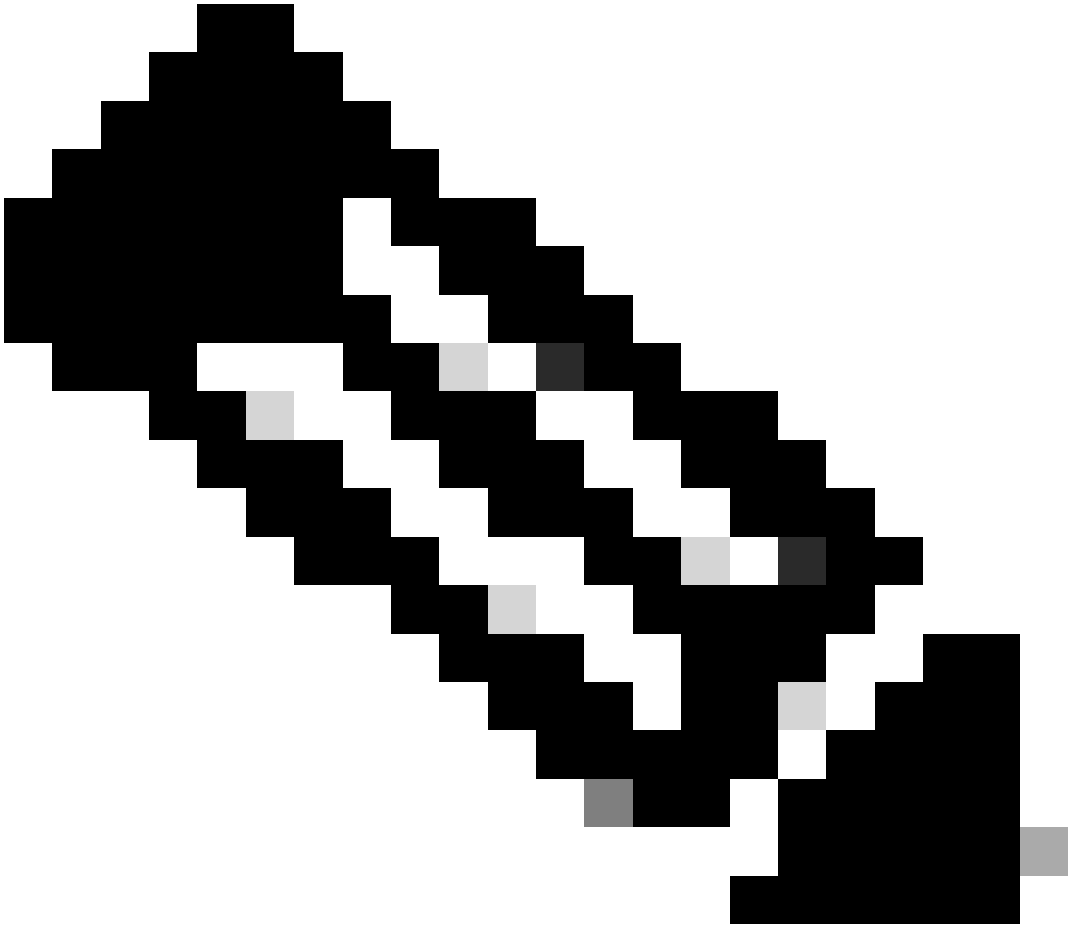
Ao configurar um ouvinte SMTP no Cisco Secure Mail, há três opções de configuração que determinam como os caracteres CR e LF expostos devem ser tratados.

Limpar mensagens de caracteres CR e LF expostos (padrão)

Com a opção padrão selecionada, o Cisco Secure Mail substitui todos os caracteres CR e LF expostos nas mensagens recebidas pela sequência correta de CRLF.

Uma mensagem com conteúdo contrabandeado, como a do exemplo, é tratada como duas mensagens separadas, e todas as verificações de segurança (como Sender Policy Framework (SPF), Autenticação de mensagens baseadas em domínio, Relatório e conformidade (DMARC),

AntiSpam, Antivírus, Proteção avançada contra malware (AMP) e filtros de conteúdo) são executadas independentemente em cada uma delas.



> Observação: os clientes devem estar cientes de que, com essa configuração, um invasor pode ser capaz de contrabandear uma mensagem representando um usuário diferente. Um invasor pode ter um impacto maior em situações em que o servidor de origem hospeda vários domínios porque o invasor pode representar um usuário de um dos outros domínios hospedados no servidor, e a verificação SPF no e-mail contrabandeado ainda passaria.

Rejeitar mensagens com caracteres CR ou LF expostos

Essa opção de configuração reforça estritamente a conformidade com o RFC. Qualquer mensagem que contenha caracteres CR ou LF expostos será rejeitada

Embora essa configuração impeça o cenário de contrabando, ela também fará com que e-mails legítimos provenientes de servidores que não são compatíveis com RFC sejam descartados.

Permitir mensagens com caracteres CR ou LF expostos (preteridos)

A configuração final faz com que o Cisco Secure Mail trate os caracteres CR e LF com seu significado ASCII. O corpo da mensagem é entregue como está, incluindo o conteúdo contrabandeado.

Como a mensagem contrabandeada é tratada como parte do corpo, os anexos incluídos como parte da mensagem contrabandeada podem não ser detectados pelo Cisco Secure Mail. Isso pode causar problemas de segurança em dispositivos downstream. Esta opção foi preterida e não deve mais ser usada.

Configuração recomendada

A Cisco recomenda o uso da opção padrão "Clean messages of bare CR and LF characters" (Limpar mensagens de caracteres CR e LF expostos), pois ela oferece o melhor compromisso entre segurança e interoperabilidade. No entanto, os clientes que usam essa configuração devem estar cientes das implicações de segurança em relação ao conteúdo contrabandeado. Os clientes que desejam aplicar a conformidade com RFC devem escolher "Reject messages with bare CR or LF characters" (Rejeitar mensagens com caracteres CR ou LF expostos), sabendo dos possíveis problemas de interoperabilidade.

Em qualquer caso, a Cisco recomenda enfaticamente a configuração e o uso de recursos como SPF, DomainKeys Identified Mail (DKIM) ou DMARC para validar o remetente de uma mensagem recebida.

As versões 15.0.2 e 15.5.2 do AsyncOS e posteriores adicionam novas funcionalidades que ajudam a identificar e filtrar mensagens que não estão em conformidade com o padrão RFC de fim de mensagem. Se uma mensagem com uma sequência de fim de mensagem inválida for recebida, o gateway de e-mail adicionará um cabeçalho de extensão X-Ironport-Invalid-End-Of-Message (cabeçalho X) a todos os IDs de mensagem (MIDs) nessa conexão até que uma mensagem que esteja em conformidade com o padrão RFC de fim de mensagem seja recebida. Os clientes podem usar um filtro de conteúdo para procurar o cabeçalho "X-Ironport-Invalid-End-Of-Message" e definir as ações a serem tomadas para essas mensagens.

Perguntas mais freqüentes

O Cisco Secure Mail é vulnerável ao ataque descrito?
Tecnicamente, sim. Quando caracteres CR e LF expostos são incluídos no e-mail, é possível que parte do e-mail seja tratada como um segundo e-mail. No entanto, como o segundo e-mail é analisado independentemente, o comportamento equivale a enviar duas mensagens separadas. A Cisco não encontrou nenhuma evidência de que o ataque descrito no artigo pudesse ser usado para ignorar qualquer um dos filtros de segurança configurados.

O documento fornece exemplos de verificações SPF e DKIM ignoradas. Por que a Cisco diz que nenhum filtro está sendo ignorado?
Nesses exemplos, as verificações SPF são executadas conforme o esperado, mas resultam em

uma verificação aprovada devido ao servidor de envio possuir vários domínios.

Qual é a configuração recomendada?
A escolha mais apropriada para um cliente depende de seus requisitos específicos. As opções recomendadas são a configuração padrão "Limpar" ou a alternativa "Rejeitar".

A escolha da opção Rejeitar resultará em falsos positivos?
A função "Rejeitar" inicia uma avaliação da adesão do e-mail aos padrões RFC. Caso o e-mail não esteja em conformidade com os padrões RFC, ele será recusado. Até mesmo e-mails legítimos podem ser rejeitados se o e-mail não estiver em conformidade com os padrões RFC.

Há um bug de software cobrindo esse problema?
A ID de bug Cisco CSCwh10142 foi arquivada.

Como posso obter mais informações sobre esse tópico?
Quaisquer perguntas de acompanhamento podem ser levantadas por meio de um caso do Technical Assistance Center (TAC).

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.