Cisco Secure Email Gateway SMTP Mikeeded Vulnerability Report에 대한 응답

목차

[소개](#)

[기술 배경](#)

[Cisco Secure Mail 동작](#)

- [Bare CR 및 LF 문자의 Clean Messages(정상 메시지)(기본값)](#)
- [Bare CR 또는 LF 문자가 포함된 메시지 거부](#)
- [Bare CR 또는 LF 문자가 포함된 메시지 허용(더 이상 사용되지 않음)](#)

[권장 컨피그레이션](#)

[자주 묻는 질문(FAQ)](#)

소개

이 문서에서는 SEC Consult에서 2023년 12월 18일에 게시한 SMTP Mikeesearching - Spoofing E-Mail Worldwide에 설명된 공격 유형에 대해 Cisco Secure Email이 어떻게 행동하는지 자세히 설명합니다.

SEC Consult Vulnerability Lab과의 공동 연구 프로젝트에서 Timo Longin(@timolongin)은 또 다른 인터넷 프로토콜인 SMTP(Simple Mail Transfer Protocol)에 대한 새로운 익스플로잇 기법을 발견했습니다. 위협 행위자는 전 세계의 취약한 SMTP 서버를 악용하여 임의의 이메일 주소에서 악성 이메일을 보내 표적 피싱 공격을 허용할 수 있습니다. 익스플로잇 자체의 특성 때문에 이러한 유형의 취약성을 SMTP 밀수라고 불렀습니다.

Cisco는 백서에 설명된 공격이 구성된 보안 필터를 우회하는 데 사용될 수 있다는 증거를 찾지 못했습니다.

기술 배경

SMTP 프로토콜 및 메시지 형식에 대해 자세히 설명하지 않고 일부 컨텍스트를 가져오기 위해 RFC 5322의 일부 섹션을 살펴보는 것이 중요합니다.

섹션 2.1은 CRLF 문자 시퀀스를 메시지의 서로 다른 섹션 간에 사용할 구분 기호로 정의합니다.

메시지는 문자 줄로 구분됩니다. 줄은 캐리지 리턴 및 라인 피드의 두 문자로 구분된 일련의 문자입니다. 즉, 캐리지 리턴(CR) 문자(ASCII 값 13) 바로 뒤에 라인 피드(LF) 문자(ASCII 값 10)가 옵니다. (캐리지 리턴/라인 피드 쌍은 일반적으로 이 문서에서 "CRLF"로 작성됩니다.)

섹션 2.3은 메시지 본문의 형식에 대해 더 자세히 설명합니다. CR과 LF 캐릭터는 결코 신체의 일부로서 독립적으로 전송되어서는 안 된다는 점을 명확히 밝히고 있다. 그렇게 하는 모든 서버는 RFC를 준수하지 않습니다.

메시지 본문은 US-ASCII 문자로 구성된 줄입니다. 본문의 유일한 두 가지 제한 사항은 다음과 같습니다.

- CR과 LF는 CRLF로만 함께 발생해야 하며, 몸에서 독립적으로 나타나서는 안 된다.
- 본문 문자의 줄은 998자로 제한해야 하며, CRLF를 제외한 78자로 제한해야 합니다.

그러나 RFC의 이전 개정판에서 사용하지 않은 구문과 관련하여 이 문서의 4.1절은 필드의 많은 구현이 올바른 구문을 사용하고 있지 않음을 인정합니다.

Bare CR과 bare LF는 서로 다른 두 가지 의미를 가진 메시지에 나타납니다. 라인 분리기를 나타내기 위해 CRLF 대신 bare CR 또는 bare LF를 부적절하게 사용하는 경우가 많다. 다른 경우, bare CR 및 bare LF는 단순히 전통적인 ASCII 의미를 갖는 US-ASCII 제어 문자로 사용됩니다.

요약하면, RFC 5322에 따르면 올바른 형식의 SMTP 메시지는 다음 예와 같습니다.

```
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
```

이 백서는 RFC 4.1 항에서 언급한 예외를 활용하여 송신 또는 수신 서버에서 보안 조치를 우회하기 위해 새로운 메시지를 본문의 일부로 삽입하거나 "밀수"하려고 시도합니다. 그 목적은 밀수된 메시지가 보안 검사를 우회하는 것인데, 이는 맨 라인이 피드되기 전에 메시지 부분에서만 검사가 실행되기 때문입니다. 예를 들면 다음과 같습니다.

<#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
```

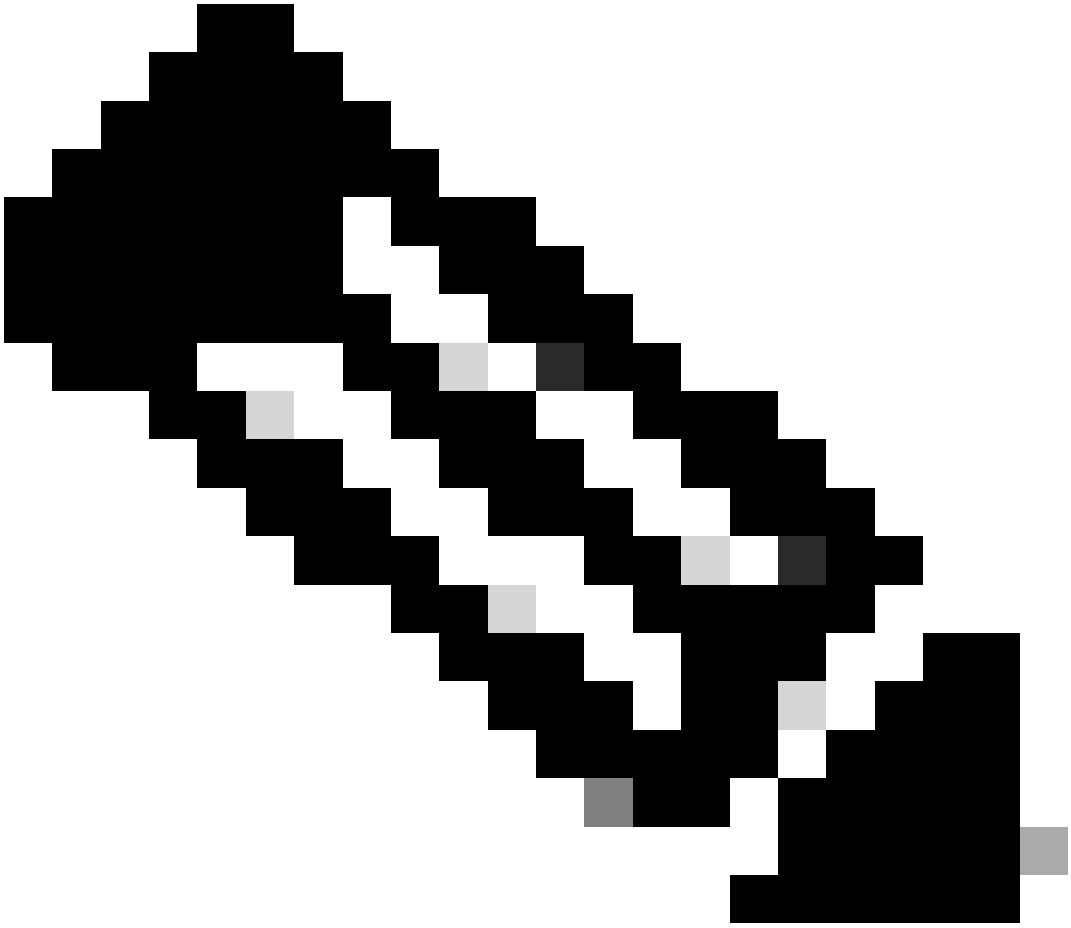
Cisco Secure Mail 동작

Cisco Secure Mail에서 SMTP 리스너를 구성할 때 기본 CR 및 LF 문자를 처리하는 방법을 결정하는 세 가지 컨피그레이션 옵션이 있습니다.

Bare CR 및 LF 문자의 Clean Messages(정상 메시지)(기본값)

기본 옵션이 선택된 경우 Cisco Secure Mail은 수신 메시지의 모든 bare CR 및 LF 문자를 올바른 CRLF 시퀀스로 교체합니다.

이 예에서와 같이 밀수된 콘텐츠가 있는 메시지는 두 개의 개별 메시지로 처리되며, 모든 보안 검사(예: SPF(Sender Policy Framework), DMARC(Domain-based Message Authentication, Reporting & Conformance), AntiSpam, Antivirus, AMP(Advanced Malware Protection) 및 콘텐츠 필터)가 각 메시지에서 독립적으로 실행됩니다.



참고: 고객은 이 컨피그레이션을 통해 공격자가 다른 사용자를 사칭하는 메시지를 밀수할 수 있다는 점을 알아야 합니다. 공격자는 서버에서 호스팅되는 다른 도메인 중 하나에서 사용자를 가장할 수 있으므로, 원래 서버가 여러 도메인을 호스팅하는 상황에서 더 큰 영향을 미칠 수 있으며, 밀수된 이메일에 대한 SPF 검사는 계속 통과하게 됩니다.

Bare CR 또는 LF 문자가 포함된 메시지 거부

이 컨피그레이션 옵션은 RFC에 대한 규정 준수를 엄격하게 적용합니다. Bare CR 또는 LF 문자가 포함된 메시지는 거부됩니다

이 컨피그레이션은 밀수 시나리오를 방지하지만, RFC 규격이 아닌 서버에서 오는 합법적인 이메일도 삭제됩니다.

Bare CR 또는 LF 문자가 포함된 메시지 허용(더 이상 사용되지 않음)

최종 컨피그레이션을 수행하면 Cisco Secure Mail에서 ASCII 의미를 갖는 베어 CR 및 LF 문자를 처리합니다. 메시지 본문은 밀수한 콘텐츠를 포함한 그대로 전달됩니다.

밀수 메시지는 본문의 일부로 처리되므로, 밀수 메시지의 일부로 포함된 첨부 파일이 Cisco Secure Mail에서 탐지되지 않을 수 있습니다. 이로 인해 다운스트림 디바이스에서 보안 문제가 발생할 수 있습니다. 이 옵션은 더 이상 사용되지 않으므로 사용할 수 없습니다.

권장 컨피그레이션

Cisco는 보안과 상호 운용성 간에 최상의 절충을 제공하므로 기본 "Clean messages of bare CR and LF characters" 옵션을 사용할 것을 권장합니다. 그러나 이 설정을 사용하는 고객은 밀수 콘텐츠와 관련된 보안 문제를 알고 있어야 합니다. RFC 규정 준수를 적용하려는 고객은 잠재적인 상호 운용성 문제를 알고 있으므로 "Reject messages with bare CR or LF characters"를 선택해야 합니다.

어떤 경우든 Cisco는 수신 메시지의 발신자를 확인하기 위해 SPF, DKIM(DomainKeys Identified Mail) 또는 DMARC와 같은 기능을 구성하고 사용할 것을 적극 권장합니다.

AsyncOS 릴리스 15.0.2 및 15.5.2 이상에서는 메시지 종료 RFC 표준을 준수하지 않는 메시지를 식별하고 필터링하는 데 도움이 되는 새로운 기능을 추가합니다. 메시지 끝 시퀀스가 잘못된 메시지가 수신되면 이메일 게이트웨이는 메시지 끝 RFC 표준을 준수하는 메시지가 수신될 때까지 해당 연결 내의 모든 메시지 ID(MID)에 X-Ironport-Invalid-End-Of-Message Extension Header(X-Header)를 추가합니다. 고객은 콘텐츠 필터를 사용하여 "X-Ironport-Invalid-End-Of-Message" 헤더를 찾고 이러한 메시지에 대해 수행할 작업을 정의할 수 있습니다.

자주 묻는 질문(FAQ)

Cisco Secure Mail은 설명된 공격에 취약합니까?
엄밀히 말하면, 그렇습니다. 메일에 bare CR 및 LF 문자가 포함된 경우, 이메일의 일부가 두 번째 이메일로 처리되도록 할 수 있습니다. 그러나 두 번째 이메일은 독립적으로 분석되므로 이 동작은 두 개의 개별 메시지를 보내는 것과 같습니다. Cisco는 백서에 설명된 공격이 구성된 보안 필터를 우회하는 데 사용될 수 있다는 증거를 찾지 못했습니다.

이 문서에서는 우회된 SPF 및 DKIM 검사의 예를 제공합니다. Cisco에서 우회되는 필터가 없다고 하는 이유는 무엇입니까?
이러한 예에서 SPF 검사는 예상대로 실행되지만, 전송 서버가 여러 도메인을 소유하기 때문에 검사에 통과됩니다.

권장되는 컨피그레이션은 무엇입니까?
고객에게 가장 적합한 선택은 고객의 특정 요구 사항에 따라 달라집니다. 권장 옵션은 기본 "Clean(정상)" 컨피그레이션 또는 "Reject(거부)" 대안입니다.

Reject(거부) 옵션을 선택하면 오탐이 발생합니까?
"거부" 기능은 이메일의 RFC 표준 준수 여부에 대한 평가를 시작합니다. 이메일이 RFC 표준을 준수하지 않을 경우 거부됩니다. 합법적인 이메일이라도 이메일이 RFC 표준을 준수하지 않을 경우 거부될 수 있습니다.

이 문제에 대한 소프트웨어 버그가 있습니까?
Cisco 버그 ID CSCwh10142가 제출되었습니다.

이 주제에 대한 자세한 내용은 어떻게 얻을 수 있습니까?
후속 질문은 TAC(Technical Assistance Center) 케이스를 통해 제기할 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.