Antwort auf den SMTP Smuggling Vulnerability Report von Cisco Secure Email Gateway

Inhalt

Einleitung

In diesem Dokument finden Sie weitere Einzelheiten zum Verhalten von Cisco Secure Email bei Angriffen, die in SMTP Smuggling - Spoofing E-Mails Worldwide, veröffentlicht am 18. Dezember 2023 von SEC Consult, beschrieben werden.

Im Rahmen eines Forschungsprojekts in Zusammenarbeit mit dem SEC Consult Vulnerability Lab entdeckte Timo Longin (@timolongin) eine neuartige Verwertungstechnik für ein weiteres Internetprotokoll - SMTP (Simple Mail Transfer Protocol). Cyberkriminelle könnten gefährdete SMTP-Server weltweit dazu missbrauchen, bösartige E-Mails von beliebigen E-Mail-Adressen aus zu versenden, was gezielte Phishing-Angriffe ermöglicht. Aufgrund der Art des Exploits selbst wurde diese Art von Sicherheitslücke als SMTP-Schmuggel bezeichnet.

Cisco hat keine Anhaltspunkte dafür gefunden, dass der im Whitepaper beschriebene Angriff verwendet werden könnte, um einen der konfigurierten Sicherheitsfilter zu umgehen.

Technischer Hintergrund

Ohne auf das SMTP-Protokoll und das Nachrichtenformat einzugehen, ist es wichtig, einige Abschnitte von RFC 5322 zu betrachten, um etwas Kontext zu erhalten.

In Abschnitt 2.1 wird die CRLF-Zeichenfolge als Trennzeichen definiert, das zwischen den verschiedenen Abschnitten der Nachricht verwendet werden soll.

Nachrichten werden in Zeichenzeilen unterteilt. Eine Zeile besteht aus einer Reihe von Zeichen, die durch die beiden Zeichen Wagenrücklauf und Zeilenvorschub, d. h. das Wagenrücklaufzeichen (CR) (ASCII-Wert 13), unmittelbar gefolgt vom Zeilenvorschub (LF)-Zeichen (ASCII-Wert 10), getrennt sind. (Das Paar aus Wagenrücklauf und Zeilenvorschub wird in diesem Dokument üblicherweise als "CRLF" geschrieben.)

In Abschnitt 2.3 wird das Format des Nachrichtentexts genauer beschrieben. Es stellt klar fest, dass CR- und LF-Zeichen niemals unabhängig als Teil des Körpers gesendet werden sollten. Server, die dies tun, sind nicht RFC-konform.

Der Text einer Nachricht besteht einfach aus Zeilen mit US-ASCII-Zeichen. Die einzigen beiden Einschränkungen auf dem Körper sind wie folgt:

- CR und LF DÜRFEN nur gemeinsam als CRLF auftreten; sie DÜRFEN NICHT unabhängig voneinander im Körper auftreten.
- Die Zeichenzeilen im Textkörper MÜSSEN maximal 998 Zeichen lang sein und SOLLTEN maximal 78 Zeichen lang sein, mit Ausnahme der CRLF.

In Abschnitt 4.1 desselben Dokuments wird jedoch in Bezug auf veraltete Syntax aus früheren, nicht so restriktiven RFC-Revisionen eingeräumt, dass viele Implementierungen in diesem Bereich nicht die richtige Syntax verwenden.

Bare CR und Bare LF erscheinen in Nachrichten mit zwei verschiedenen Bedeutungen. In vielen Fällen werden bloße CR oder bloße LF nicht korrekt anstelle von CRLF verwendet, um Trennlinien anzugeben. In anderen Fällen werden nackte CR und nackte LF einfach als US-ASCII-Kontrollzeichen mit ihren traditionellen ASCII-Bedeutungen verwendet.

Zusammenfassend lässt sich sagen, dass eine ordnungsgemäß formatierte SMTP-Nachricht gemäß RFC 5322 wie das folgende Beispiel aussieht:

```
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
```

Das Papier versucht, die in Abschnitt 4.1 der RFC genannte Ausnahme zu nutzen, um eine neue Nachricht als Teil des Hauptteils einzufügen oder zu "schmuggeln", um Sicherheitsmaßnahmen auf dem sendenden oder empfangenden Server zu umgehen. Ziel ist es, dass die geschmuggelte Nachricht die Sicherheitsüberprüfungen umgeht, da diese Überprüfungen nur für den Teil der Nachricht ausgeführt würden, bevor die reinen Nachrichtenfeeds ausgeführt werden. Beispiele:

<#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

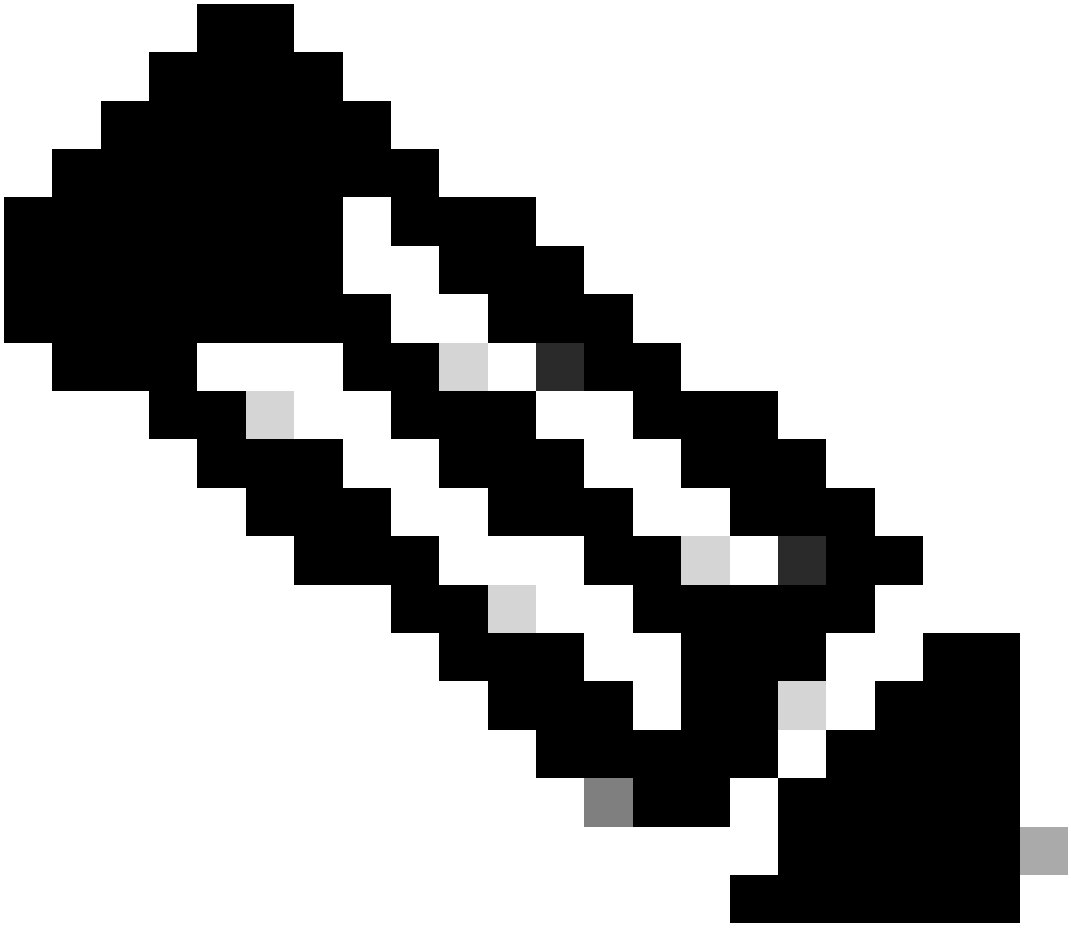
Cisco Secure Mail-Verhalten

Bei der Konfiguration eines SMTP-Listeners in Cisco Secure Mail gibt es drei Konfigurationsoptionen, die festlegen, wie bloße CR- und LF-Zeichen behandelt werden sollen.

Nachrichten mit Bare-CR- und -LF-Zeichen löschen (Standard)

Wenn die Standardoption aktiviert ist, ersetzt Cisco Secure Mail alle Bare-CR- und -LF-Zeichen in eingehenden Nachrichten mit der richtigen CRLF-Sequenz.

Eine Nachricht mit geschmuggeltem Inhalt, wie im Beispiel, wird als zwei separate Nachrichten behandelt, und alle Sicherheitsprüfungen (wie Sender Policy Framework (SPF), Domain-based Message Authentication, Reporting & Conformance (DMARC), AntiSpam, Antivirus, Advanced Malware Protection (AMP) und Content-Filter) werden unabhängig auf jedem von ihnen ausgeführt.



Hinweis: Kunden sollten sich bewusst sein, dass ein Angreifer mit dieser Konfiguration möglicherweise in der Lage ist, eine Nachricht zu schmuggeln, die einen anderen Benutzer imitiert. Ein Angreifer könnte größere Auswirkungen in Situationen haben, in denen der Ursprungsserver mehrere Domänen hostet, da der Angreifer die Identität eines Benutzers einer der anderen Domänen übernehmen könnte, die auf dem Server gehostet werden, und die SPF-Prüfung der geschmuggelten E-Mail dennoch erfolgreich war.

Nachrichten mit Bare-CR- oder -LF-Zeichen ablehnen

Mit dieser Konfigurationsoption wird die Einhaltung der RFC-Richtlinien streng durchgesetzt. Alle Nachrichten mit Bare-CR- oder -LF-Zeichen werden abgelehnt.

Diese Konfiguration verhindert zwar das Schmuggeln, führt aber auch dazu, dass legitime E-Mails von Servern, die nicht RFC-konform sind, verworfen werden.

Nachrichten mit Bare-CR- oder -LF-Zeichen zulassen (veraltet)

Nach der letzten Konfiguration behandelt Cisco Secure Mail bloße CR- und LF-Zeichen mit ihrer ASCII-Bedeutung. Der Nachrichtentext wird wie besehen übermittelt, einschließlich des geschmuggelten Inhalts.

Da die geschmuggelte Nachricht als Teil des Textkörpers behandelt wird, werden Anlagen, die Teil der geschmuggelten Nachricht sind, von Cisco Secure Mail möglicherweise nicht erkannt. Dies kann Sicherheitsprobleme auf Downstream-Geräten verursachen. Diese Option ist veraltet und sollte nicht mehr verwendet werden.

Empfohlene Konfiguration

Cisco empfiehlt die Verwendung der Standardoption "Nachrichten reinigen mit Bare-CR- und LF-Zeichen", da diese den besten Kompromiss zwischen Sicherheit und Interoperabilität bietet. Kunden, die diese Einstellung verwenden, sollten sich jedoch der Auswirkungen bewusst sein, die Schmuggelinhalte auf die Sicherheit haben. Kunden, die die RFC-Konformität durchsetzen möchten, sollten unter Berücksichtigung potenzieller Interoperabilitätsprobleme die Option "Reject messages with bare CR or LF characters" (Nachrichten mit Bare-CR- oder -LF-Zeichen ablehnen) wählen.

In jedem Fall empfiehlt Cisco dringend, Funktionen wie SPF, DomainKeys Identified Mail (DKIM) oder DMARC zu konfigurieren und zu verwenden, um den Absender einer eingehenden Nachricht zu validieren.

AsyncOS, Versionen 15.0.2 und 15.5.2 und höher, fügen neue Funktionen hinzu, mit denen Nachrichten identifiziert und gefiltert werden können, die nicht dem RFC-Standard für das Ende einer Nachricht entsprechen. Wenn eine Nachricht mit einer ungültigen Ende-der-Nachricht-Sequenz empfangen wird, fügt das E-Mail-Gateway allen Nachrichten-IDs (MIDs) innerhalb dieser Verbindung einen X-IronPort-Invalid-End-of-Message Extension Header (X-Header) hinzu, bis eine Nachricht empfangen wird, die dem Ende-der-Nachricht-RFC-Standard entspricht. Kunden können einen Content-Filter verwenden, um nach dem Header "X-IronPort-Invalid-End-Of-Message" zu suchen und die für diese Nachrichten durchzuführenden Aktionen zu definieren.

Häufig gestellte Fragen

Ist Cisco Secure Mail anfällig für den beschriebenen Angriff?
Technisch gesehen ja. Wenn bloße CR- und LF-Zeichen in der E-Mail enthalten sind, kann es passieren, dass ein Teil der E-Mail als zweite E-Mail behandelt wird. Da die zweite E-Mail jedoch unabhängig analysiert wird, entspricht das Verhalten dem Senden zweier separater Nachrichten. Cisco hat keine Anhaltspunkte dafür gefunden, dass der im Whitepaper beschriebene Angriff verwendet werden könnte, um einen der konfigurierten Sicherheitsfilter zu umgehen.

Das Whitepaper enthält Beispiele für umgangene SPF- und DKIM-Prüfungen. Warum sagt Cisco, dass keine Filter umgangen werden?
In diesen Beispielen werden SPF-Prüfungen erwartungsgemäß ausgeführt, führen jedoch zu einer übergebenen Prüfung, da der sendende Server über mehrere Domänen verfügt.

Welche Konfiguration wird empfohlen?

Die für einen Kunden am besten geeignete Wahl hängt von seinen spezifischen Anforderungen ab. Die empfohlenen Optionen sind entweder die Standardkonfiguration "Clean" oder die Alternative "Reject" (Ablehnen).

Führt die Auswahl der Option Ablehnen zu Fehlalarmen?
Die Funktion "Reject" (Ablehnen) prüft, ob die E-Mail den RFC-Standards entspricht. Falls die E-Mail nicht den RFC-Standards entspricht, wird sie abgelehnt. Selbst legitime E-Mails können abgelehnt werden, wenn die E-Mail nicht den RFC-Standards entspricht.

Gibt es einen Softwarefehler, der dieses Problem behebt?
Cisco Bug-ID CSCwh10142 wurde abgelegt.

Wie erhalte ich weitere Informationen zu diesem Thema?
Bei weiteren Fragen können Sie ein Ticket beim Technical Assistance Center (TAC) erstellen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.