Antwoord op het kwetsbaarheidsrapport van Cisco Secure Email Gateway voor Smuggling

Inhoud

Inleiding

Technische achtergrond

Cisco Secure Mail-gedrag

- Berichten over tekens voor onbewerkte tekens op de tekenherkenning en de tekenherkenning reinigen (standaard)
- Berichten met duidelijke tekens van OCR of LF afwijzen
- Berichten met duidelijke tekens van OCR of LF toestaan (afgekeurd)

Aanbevolen configuratie

Veelgestelde vragen

Inleiding

Dit document bevat meer informatie over de manier waarop Cisco Secure Email zich gedraagt tegen het type aanval dat wordt beschreven in Smuggling - Spoofing E-Mails Worldwide, gepubliceerd op 18 december 2023 door SEC Consult.

In de loop van een onderzoeksproject, in samenwerking met het SEC Consult Vulnerability Lab, ontdekte Timo Longin (@timolongin) een nieuwe exploitatietechniek voor weer een nieuw internetprotocol - SMTP (Simple Mail Transfer Protocol). Bedreigingsactoren kunnen over de hele wereld misbruik maken van kwetsbare SMTP-servers om kwaadaardige e-mails te versturen van willekeurige e-mailadressen, waardoor gerichte phishing-aanvallen mogelijk worden. Vanwege de aard van de uitbuiting zelf, werd dit type van kwetsbaarheid genoemd SMTP smokkel.

Cisco heeft geen bewijs gevonden dat de aanval die in het papier wordt beschreven, zou kunnen worden gebruikt om een van de geconfigureerde beveiligingsfilters te omzeilen.

Technische achtergrond

Zonder in detail te treden over het SMTP-protocol en het berichtenformaat, is het belangrijk om een aantal secties van RFC 5322 te bekijken om enige context te krijgen.

In punt 2.1 wordt de tekensequentie van het CRLF gedefinieerd als het scheidingsteken dat tussen de verschillende delen van het bericht moet worden gebruikt.

De berichten worden in regels tekens verdeeld. Een lijn is een reeks tekens die wordt afgebakend door de twee tekens wagenterugloop en line-feed; dat wil zeggen het wagenterugloop (CR)-teken (ASCII-waarde 13), onmiddellijk gevolgd door het lijninvoerteken (LF) (ASCII-waarde 10). (Het paar van het vervoerterugkeer/van de lijnvoer wordt gewoonlijk geschreven in dit document als "CRLF".)

Punt 2.3 betreft de vorm van de berichttekst. Het geeft duidelijk aan dat CR- en LF-tekens nooit onafhankelijk als deel van het lichaam mogen worden verzonden. Een server die dit doet, is niet compatibel met de RFC.

De hoofdtekst van een bericht bestaat uit regels met tekens uit de US-ASCII. De enige twee beperkingen op het lichaam zijn:

- CR en LF MOGEN alleen samen voorkomen als CRLF; ze MOGEN NIET los van elkaar in het lichaam voorkomen.
- De lijnen van karakters in het lichaam MOETEN tot 998 karakters worden beperkt, en ZOUDEN tot 78 karakters, met uitzondering van CRLF moeten worden beperkt.

Paragraaf 4.1 van datzelfde document erkent echter, met betrekking tot de verouderde syntaxis van eerdere herzieningen van de RFC die niet zo restrictief waren, dat veel implementaties op het veld niet de juiste syntaxis gebruiken.

Bare CR en naakte LF verschijnen in berichten met twee verschillende betekenissen. In veel gevallen worden kale CR of kale LF onjuist gebruikt in plaats van CRLF om lijnscheidingstekens aan te geven. In andere gevallen worden alleen "bare CR" en "bare LF" gebruikt om Amerikaanse en ASCII-personages te controleren met hun traditionele ASCII-betekenissen.

Samenvattend, volgens RFC 5322, zou een behoorlijk geformatteerd SMTP bericht als het volgende voorbeeld kijken:

```
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
```

Het artikel probeert de uitzondering die in paragraaf 4.1 van de RFC wordt genoemd, te gebruiken om een nieuw bericht in te voegen of te "smokkelen" als deel van het document, in een poging om de beveiligingsmaatregelen op de verzendende of ontvangende server te omzeilen. Het doel is dat het gesmokkelde bericht de veiligheidscontroles omzeilt, omdat die controles alleen worden uitgevoerd op het deel van het bericht dat wordt verzonden voordat de blote lijn wordt gevoed. Voorbeeld:

<#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-gedrag

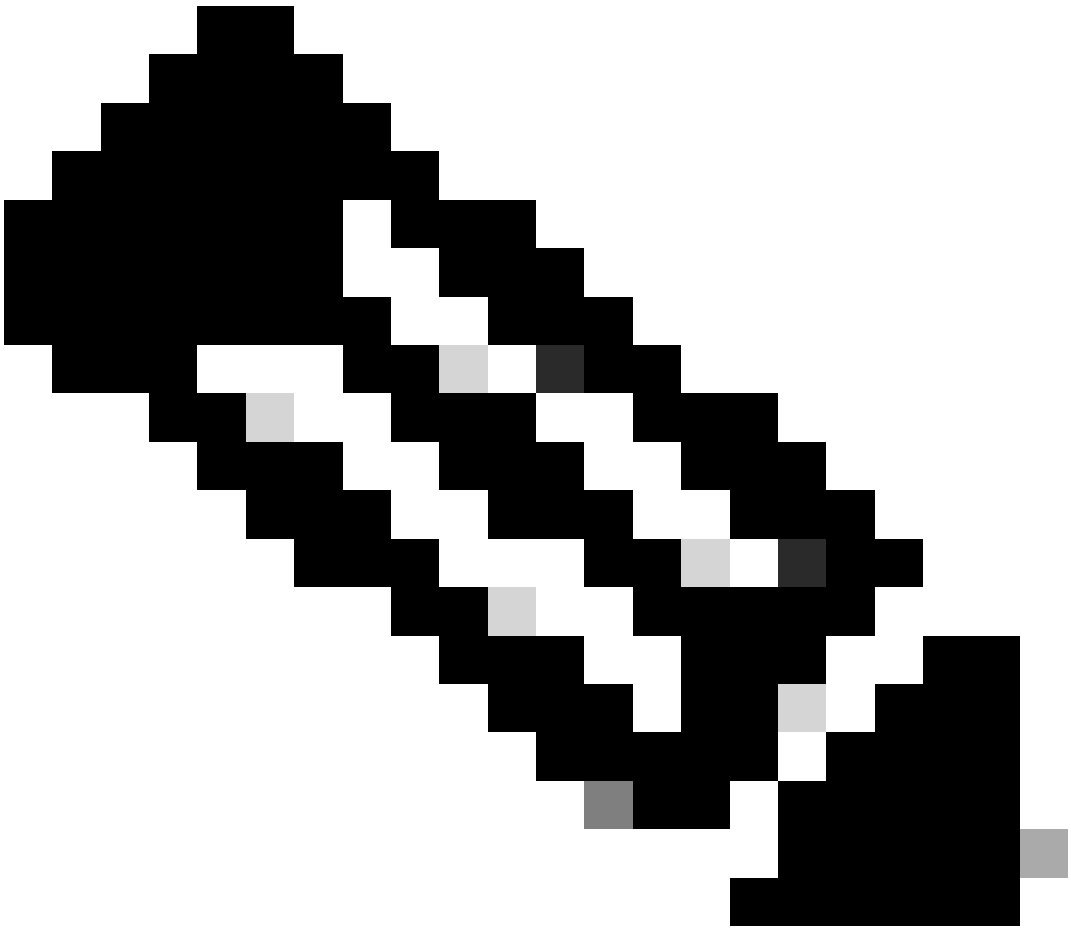
Bij het configureren van een SMTP-luisteraar op Cisco Secure Mail zijn er drie configuratieopties die bepalen hoe kale CR- en LF-tekens moeten worden behandeld.

Berichten over tekens voor onbewerkte tekens op de tekenherkenning en de tekenherkenning reinigen (standaard)

Als de standaardoptie is geselecteerd, vervangt Cisco Secure Mail alle naakte CR- en LF-tekens in inkomende berichten door de juiste CRLF-reeks.

Een bericht met gesmokkelde inhoud, zoals in het voorbeeld, wordt behandeld als twee afzonderlijke berichten, en alle veiligheidscontroles (zoals het Kader van het Beleid van de Afzender (SPF), op Domein-Gebaseerde Verificatie van het Bericht, Rapportage & Conformiteit (DMARC), AntiSpam, Antivirus, Geavanceerde Bescherming van Malware (AMP), en

inhoudsfilters) worden in werking gesteld onafhankelijk op elk van hen.



> Opmerking: Klanten moeten zich ervan bewust zijn dat een aanvaller met deze configuratie een bericht kan smokkelen dat een andere gebruiker imiteert. Een aanvaller kan een grotere impact hebben in situaties waar de oorspronkelijke server meerdere domeinen host, omdat de aanvaller een gebruiker kan imiteren van een van de andere domeinen die worden gehost op de server, en de SPF controle van de gesmokkelde e-mail zou nog steeds overgaan.

Berichten met duidelijke tekens van OCR of LF afwijzen

Deze configuratieoptie dwingt strikte naleving van de RFC af. Alle berichten met alleen CR- of LF-tekens worden afgewezen

Hoewel deze configuratie het smokkelscenario voorkomt, zal het ook veroorzaken dat legitieme e-mails die afkomstig zijn van servers die niet RFC-compatibel zijn worden gedropt.

Berichten met duidelijke tekens van OCR of LF toestaan (afgekeurd)

De definitieve configuratie zorgt ervoor dat Cisco Secure Mail kale CR- en LF-tekens met hun ASCII-betekenis behandelt. De berichttekst wordt geleverd in de huidige staat, inclusief de gesmokkelde inhoud.

Omdat het gesmokkelde bericht wordt behandeld als deel uitmakend van de inhoud, worden bijlagen die als deel van het gesmokkelde bericht zijn opgenomen mogelijk niet herkend door Cisco Secure Mail. Dit zou veiligheidskwesties op stroomafwaartse apparaten kunnen veroorzaken. Deze optie is afgekeurd en dient niet langer te worden gebruikt.

Aanbevolen configuratie

Cisco raadt het gebruik van de standaard "Schone berichten met naakte CR en LF tekens" optie aan omdat dit het beste compromis biedt tussen beveiliging en interoperabiliteit. Klanten die deze instelling gebruiken, dienen zich echter bewust te zijn van de veiligheidsimplicaties met betrekking tot gesmokkelde inhoud. Klanten die naleving van RFC willen afdwingen, moeten kiezen voor "Afwijzen van berichten met naakte CR of LF tekens", zich bewust van de potentiële interoperabiliteitsproblemen.

In elk geval raadt Cisco sterk aan functies te configureren en te gebruiken zoals SFP, DomainKeys Identified Mail (DKIM) of DMARC om de verzender van een inkomend bericht te valideren.

AsyncOS geeft 15.0.2 en 15.5.2 uit en voegt later nieuwe functionaliteit toe die helpt om berichten te identificeren en te filteren die niet voldoen aan de end-of-message RFC-standaard. Als een bericht met een ongeldige eind-van-bericht opeenvolging wordt ontvangen, voegt de e-mailgateway een X-Ironport-Invalid-End-Of-Message Extension Header (X-Header) toe aan al bericht IDs (MIDs) binnen die verbinding tot een bericht dat aan de eind-van-bericht RFC-norm voldoet wordt ontvangen. Klanten kunnen een content filter gebruiken om te zoeken naar de "X-Ironport-Invalid-End-Of-Message" header en om de handelingen te definiëren die voor deze berichten moeten worden uitgevoerd.

Veelgestelde vragen

Is Cisco Secure Mail kwetsbaar voor de beschreven aanval?
Technisch gezien wel. Als er alleen CR- en LF-tekens in de e-mail worden opgenomen, is het mogelijk dat een deel van de e-mail als een tweede e-mail wordt behandeld. Aangezien de tweede e-mail echter onafhankelijk wordt geanalyseerd, is het gedrag gelijk aan het verzenden van twee afzonderlijke berichten. Cisco heeft geen bewijs gevonden dat de aanval die in het papier wordt beschreven, zou kunnen worden gebruikt om een van de geconfigureerde beveiligingsfilters te omzeilen.

Het artikel bevat voorbeelden van niet via SPF- en DKIM-controles uitgevoerde controles.
Waarom zegt Cisco dat er geen filters worden overgeslagen?
In die voorbeelden, worden de SPF-controles uitgevoerd zoals verwacht, maar resulteren in een

doorgegeven controle doordat de verzendende server meerdere domeinen bezit.

Wat is de aanbevolen configuratie?
De meest geschikte keuze voor een klant is afhankelijk van hun specifieke vereisten. De aanbevolen opties zijn de standaard "Clean"-configuratie of het alternatief "Reject".

Zal het kiezen van de optie Afwijzen resulteren in valse positieven?
De "Reject" functie start een beoordeling van de naleving van de RFC standaarden door de e-mail. In het geval dat de e-mail niet voldoet aan de RFC-standaarden, zal deze worden geweigerd. Zelfs legitieme e-mails kunnen worden geweigerd als de e-mail niet voldoet aan de RFC-normen.

Is er een softwarebug die dit probleem behandelt?
Cisco bug-id CSCwh10142 is ingediend.

Hoe kan ik meer informatie over dit onderwerp krijgen?
Alle vervolgvragen kunnen worden gesteld via een TAC-case (Technical Assistance Center).

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.