

Secure Firewall FTD - Zoom Phone Audio Blocklist Vanwege oudere VDB

Inhoud

uitgifte

Gebruikers ervaren audioproblemen met zoomtelefoongesprekken waarbij oproepen verbinding maken, maar audio ontbreekt. De FTD laat UDP-mediapakketten vallen uit Zoom IP-reeksen en toont ze als geblokkeerd door Snort in pakketopnamen en ASP-droptellers.

Specifieke symptomen waren onder meer:

- In de firewall wordt Cisco Vulnerability Database (VDB) versie 427 of ouder uitgevoerd.
- De firewall bevat een toegangsregel die zoomverkeer moet toestaan op basis van de standaard Zoom/RTP-applicatie-ID's die door de Firepower-database worden verstrekt. De regel moet al deze poorten toestaan via de Zoom AppID's, volgens appid.cisco.com:
 - Gebruikerszoom (6243): 80,443/tcp
 - Zoomdownload (4628): 80,443/tcp
 - Zoom Upload (4627): 80,443/tcp
 - Zoomvergadering (4629): 80/tcp
 - RTP-audio (2475): 5004/udp
 - SIP (426): 5060/UDP
- Uit de packet-tracer-uitvoer blijkt echter dat het verkeer wordt gedropt om de reden van de blokkeerlijst "Geblokkeerd of op de zwarte lijst geplaatst door de firewall-preprocessor".

<#root>

Phase: 17
Type: SNORT
Subtype: firewall

Result: DROP

Elapsed time: 345716 ns

Config:

Network 0, Inspection 0, Detection 4, Rule ID 268434438

Additional Information:

Starting rule matching, zone 3 -> 3, geo 840 -> 840, vlan 0, src sgt: 0, src sgt type: unknown, ds

Matched rule ids 268434438 - Block

Result:

input-interface: Outside(vrfid:0)

input-status: up

input-line-status: up

output-interface: Outside(vrfid:0)

output-status: up

output-line-status: up

Action: drop

Time Taken: 640578 ns

Drop-reason: (firewall) Blocked or blacklisted by the firewall preprocessor, Drop-location: frame

- Packet captures tonen druppels met reden: "snort-blacklist".

<#root>

40: 22:52:36.383692 206.247.118.57.60030 > 10.X.X.1.9178: udp 103

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA

141: 22:52:36.383723 206.247.118.57.60030 > 10.X.X.1.9178: udp 103

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA

142: 22:52:36.385188 206.247.118.57.60030 > 10.X.X.1.9178: udp 44

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA

- Bij traceeroutputs voor systeemondersteuning wordt het verkeer uitgesteld tijdens het matchen van regels vanwege de identificatie van de toepassing in behandeling. Het verkeer wordt echter verkeerd geïdentificeerd en geblokkeerd. IP-adres is een openbaar Zoom-IP-adres waarvoor toegang vereist is volgens de Zoom-[artikel Zoom-netwerfirewall of proxyserverinstellingen](#).

<#root>

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

pending rule order 12, 'allow-outbound', AppID

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

Deferring trust until a rule is matched

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

match rule order 28, 'Default Block', action Block

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 MidRecovery data sent for rule id: 26843

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Matched a rule, stop deferring trust

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Generating an SOF event with rule_id = 2

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

deny action

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Deleting Firewall session flags=0x20, 1c

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Packet 17168248: UDP, 04/14-14:44:53.110

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Firewall: starting rule matching, zone 1

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

Firewall: block rule, 'Default Block', force_block

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

AppID: service: (-1), client: (0), payload: (0), misc: (0)

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Stream: pending block, drop

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Policies: Network 0, Inspection 0, Detect

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

Verdict: blacklist

- Systeemondersteuningssporen geven "RTP-client candidate returned error-invalid (-11)" en "3rd party returned unknown (0)" berichten aan wanneer Zoom-IP's proberen te reageren.

<#root>

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1 New AppId session

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1

3rd party returned unknown (0)

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1

RTP client candidate returned error-invalid (-11)

10.X.X.1 9824 -> 206.247.118.55 54808 17 AS=0 ID=2 GR=1-1 app event changes: created

- FTD-show asp drop commando toont een snelle toename van de blacklist drops.

<#root>

Frame drop:

-----ABBREVIATED-----

Blocked or blacklisted by the firewall preprocessor (firewall)	11224
Blocked or blacklisted by the stream preprocessor (stream)	2354
Fragment reassembly failed (fragment-reassembly-failed)	3
Packet is blacklisted by snort (snort-blacklist)	27173
Packet is blocked as requested by snort (snort-block)	42

milieu

- Cisco Firepower FTD versie 7.7.11 beheerd door FMC
- Vulnerability Database (VDB) versie 427 of ouder
- Snort versie 3.3.5.1100-66
- Verkeer dat voornamelijk van invloed is op Zoom IP-subnetten 170.114.0.0/16 en 206.247.0.0/16, maar kan ook andere Zoom IP's bevatten

resolutie

Cisco bug ID CSCwu22106 Workaround - Implementatie van voorfilterregel

1: Maak een voorfilterregel voor het zoomverkeer.

Navigeer naar Beleid > Toegangsbeheer > Voorfilter en maak een nieuwe regel met deze configuratie:

- Regelnaam: Zoom-Prefilter
- Actie: FastPath
- Bronzone: INVOERINTERFACE
- Bestemmingszone: OUTPUTINTERFACE
- Bronadres: alle
- Bronpoort: alle
- Bestemmingsadres: Zoom IP-bereiken (170.114.0.0/16, 206.247.0.0/16) en alle andere die worden vermeld in [Zoom-netwerkfirewall- of proxyserverinstellingen](#).
- Poort van bestemming: UDP 10000-64000

2: Configuratie van alternatieve toegangscontroleregels

Als prefiltering niet de voorkeur heeft, wijzigt u de bestaande regel voor het toegangsbeheerbeleid door Zoom-toepassings-id's te verwijderen en expliciete IP- en poortmatching te gebruiken:

- Regelnaam: Zoom-Allow
- Actie: toestaan
- Bronzone: INVOERINTERFACE
- Bestemmingszone: OUTPUTINTERFACE
- Bronadres: alle
- Bronpoort: alle
- Bestemmingsadres: Zoom IP-bereiken (170.114.0.0/16, 206.247.0.0/16) en alle andere die worden vermeld in [Zoom-netwerkfirewall- of proxyserverinstellingen](#).
- Bestemmingspoort: UDP / "Zoom-Phone-Ports" (bereik 10000 64000)
- Logboekregistratie: (optioneel, voor het bewaken van toegestaan verkeer)

3: Implementeer de configuratiewijzigingen op de FTD-apparaten en controleer of de tweeweg-audiofunctionaliteit is hersteld.

- Controleer de valtelers van ASP om te bevestigen dat de blokkering is gestopt:

```
device# show asp drop
```

- Controleer pakketopnames voor succesvol bidirectioneel verkeer:

```
device# show capture
```

4: Defect Cisco bug ID CSCwu22106 werd opgelost in de release van Cisco Vulnerability Database (VDB) versie 428. Firepower-apparaten moeten de nieuwste VDB-versies uitvoeren om impact van dit defect te voorkomen. Evenzo werd het gerelateerde defect Cisco bug ID CSCwn80786 opgelost in VDB versie 395.

Oorzaak

Een defect in de identificatiehandtekeningen van de Cisco Secure Firewall-applicatie binnen Vulnerability Database (VDB) versie 427 zorgt ervoor dat Zoom Phone-mediaverkeer verkeerd wordt geclassificeerd en vervolgens wordt geblokkeerd door de Snort-inspectiemachine. Dit gedrag wordt bijgehouden onder Cisco bug ID CSCwu22106 en gerelateerd defect Cisco bug ID CSCwn80786, die een onjuiste verwerking van Zoom IP-adressen en mediastromen documenteert wanneer applicatie-ID's worden gebruikt.

Gerelateerde inhoud

- [Instellingen voor netwerkfirewall of proxyserver zoomen](#)
- [Best practices voor fastpath prefiltering](#)
- [Cisco bug ID CSCwu22106 - Zoom IP-adressen onjuist behandeld in VDB 427](#)
- [Cisco bug ID CSCwn80786 - Zoom applicatie detector detecteert geen netwerken voor zoom telefoon](#)
- [Cisco Technical Support en downloads](#)

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.